TAMPEREEN TEKNILLINEN YLIOPISTO

MIKA NORRGÅRD

VERKON HAVAINNOINTI HUNAJAPURKEILLA JA TUNKEUTUMISEN HAVAITSEMISJÄRJESTELMÄLLÄ

Diplomityö

Tarkastajat: Professori Pekka Loula, diplomi-insinööri Matti Monnonen
Tarkastajat ja aihe hyväksytty Tuotantotalouden ja rakentamisen tiedekuntaneuvoston kokouksessa 15. toukokuuta 2013

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO, PORIN YKSIKKÖ
Tietotekniikan koulutusohjelma
NORRGÅRD, MIKA: Verkon havainnointi hunajapurkeilla ja tunkeutumisen havaitsemisjärjestelmällä.
Diplomityö, 70 sivua, 8 liitesivua
Kesäkuu 2013
Pääaine: Tietoliikennetekniikka
Tarkastajat: Professori Pekka Loula, diplomi-insinööri Matti Monnonen
Avainsanat: Hunajapurkki, tunkeutumisen havaitseminen, tietoturva, tarkkailu, verkkoliikenne, verkko

Tietoturvallisuuden tärkeys kasvaa jatkuvasti kiihtyvällä vauhdilla. Pienien kannettavien päätelaitteiden yleistyessä niitä isännöivien verkkojen suojaaminen tulee haastavaksi ja on pyrittävä yhdistelemään yhä erilaisempia suojautumistekniikoita hyökkääjien havaitsemiseksi. Hunajapurkit toimivat verkossa hyökkäyksiä havaitsevina sensoreina. Koska ne esiintyvät verkossa yhtenä verkon koneista, niihin usein kohdistuu verkon skannaukset ja sellaiset yhteydenotot, jotka verkkoon eivät kuulu. Hunajapurkit asetetaan yleensä sellaisiin IP-osoitteisiin tai IP-avaruuteen, jotka eivät ole käytössä. Tällöin voidaan kaikki sille saapuva liikenne laskea epäilyttäväksi. Liikenteestä kerättyjä lokitietoja voidaan yhdistellä verkon muiden havainnointijärjestelmien kanssa tarkemman ymmärryksen saavuttamiseksi.

Tutkimuksessa pyrittiin testaamaan Honeyd-hunajapurkkeja ja tunkeutumisen havaitsemisjärjestelmä Snortia verkon tarkkailussa. Hunajapurkit ja tunkeutumisen havaitsemisjärjestelmä yhdistettiin keskittimeen, joka vuorollaan yhdistettiin viiteen erilaiseen verkkorakenteeseen. Näistä viidestä tapauksesta yksi oli sisäverkosta tapahtuvan hyökkäyksen havainnointia, yksi oli ADSL-yhteyden kautta tulevan liikenteen havainnointia ja kolme oli matkapuhelinverkon kautta tulevan liikenteen havainnointia. Matkapuhelinverkon kautta tulleet tapaukset erosivat toisistaan sillä, että ensimmäisessä havainnointiin DMZ-alueelle tullutta liikennettä, toisessa havainnoitiin virtuaalipalvelimen verkkoon ohjaamaa liikenttä ja kolmannessa luotiin kolmen hunajapurkin hunajaverkko, jolle liikenne ohjattiin.

Tutkimus osoittaa, että hunajapurkit tuovat hyvän lisän verkon tunkeutumisen havaitsemiseen. Niiden avulla saadaan liikennöinnistä sellaista tietoa, joka saattaa jäädä muilla tavoin verkkoa tarkkailevilta menetelmiltä huomaamatta.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Information Technology
NORRGÅRD, MIKA: Observing the network using honeypots and a intrusion detection system
Master of Science Thesis, 70 pages, 8 Appendix pages
June 2013
Major: Communications engineering
Examiner: Professor Pekka Loula, M.Sc.(Tech.) Matti Monnonen
Keywords: Honeypot, intrusion detection, computer security, network traffic, Honeyd, Snort

The importance of computer security is constantly growing and as the amount an divercity of small devices equipped with networking capabilty is multiplying, the need to be able to protect these networks is also growing. A good way to do this is to combine different types of techniques to catch possible intruders. Honeypots act as sensors in a network. They appear to an intruder as normal devices in a network. Because of that they can get targeted by network scans and connections that do not belong to the normal activities of protected netwok. Honeypots are usually placed into IP-addresses or networksegment that are not in use and normally would not receive any traffic. That's why all traffic directed at them can be conseidered to be suspicious. By combining the information collected by honeypots and other intrusion detection systems we can gain better understanding of the attacks and use it to further strengthen our network security.

The objective of this thesis is to study the use of Honeyd honeypots in combination with Snort intrusion detection system as tools to observe the network. Honeypots and itrusion detection systen were connected to a hub that in turn was connected to five different network-cases. These were the detection of an attack in the internal network of an organisation, the detection of the traffic in a network connected to the Internet through ADSL-connection, the detection of the traffic in a network connected to the Internet through mobile phone network, the detection of traffic in a network with connections being routed by a virtualserver and the detection of traffic in a network with multiple honeypots in it.

This thesis shows that honeypots can be an asset in detecting intrusions. They can add to the effienciency of an intrusion detection system by providing a different view to the network traffic.

ALKUSANAT

Diplomityö tehtiin Tampereen teknilliselle yliopistolle. Kiitokseni professori Pekka Loulalle ja diplomi-insinööri Matti Monnoselle työn ohjaamisesta ja sen tarkistamisesta. Lopuksi haluan kiittää perhettäni tuesta työn ja opiskelujen aikana.

Porissa 17.5.2013

Mika Norrgård

SISÄLLYS

TERMIT JA NIIDEN MÄÄRITELMÄT

ADSL-yhteys	Verkkokyrkentätekniikka, joka mahdollistaa nopean tietoliikenteen puhelinlinjoja pitkin.
Aktiivinen järjestelmä	Verkon havainnointijärjestelmä, joka muokkaa tai estää havainnoimaansa tietoa.
Alkuperäiset lokitiedostot	Lokitiedostot, joita laitteet ja ohjelmat luovat toiminnastaan.
Allekirjoitusten havainnointi	Tapahtuma, jossa havainnoidaan tietty kuvio pakettiliikenteen otsakkeissa tai käyttäytymisessä.
ARP	Address Resolution Protocol. Protokolla, jonka avulla selvitetään MAC-osoite.
ARP-väärennös	ARP-viestien hyväksikäyttöhyökkäys. Mahdollistaa hyökkääjän asettumisen tietoliikenteen välittäjäksi.
Barnyard2	Snort unifed2-tiedoston tulkki.
Chroot Jail	Rajattu alue tiedostojärjestelmässä, jonne epäturvallinen ohjelma voidaan asentaa.
Context Management	Dynaaminen tietokoneprosessi, jolla voidaan kohdistaa sen alaisuudessa olevien ohjelmien sisältö tiettyyn aihealueeseen.
DD-WRT	Linux-pohjainen ohjelmisto langattomille reittimille.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jota käytetään jakamaan verkkoon liittyville laitteille IP-osoiteet.
DMZ	Demilitarized zone. Aliverkko, joka yhdistää sisäverkon turvattomaan alueeseen, kuten Internetiin.
DNS	Domain Name System. Nimipalvelu, jonka avulla Internetiin liittyneet tietokoneet voivat käyttää verkkotunnuksia IP-osoitteiden sijasta.
DoS	Palvelunestohyökkäys, joka on yritys kaataa tai lamauttaa palvelu.
Dynaamiset säännöt	Vulnerability Research Team-ryhmän määrittelemät säännöt tunkeutumisen havaitsemisjärjestelmä Snortin toiminnalle. Niiden perusteella Snort tietää milloin sen kuuluu antaa hälytys.
Echo-viesti	Viesti, jolla testataan laitteen saavutettavuutta.
Etäkäyttöpalvelu	Sallii laitteen käyttämisen verkon kautta.

Farpd	Ohjelma, joka vastaa ARP-pyyntöihin määritellyn verkkoliitännän MAC-osoitteella.
FTP	File Transfer Protocol. Tiedostonsiirtomenetelmä tietokoneiden välille.
Gnu GPL-lisenssi	Gnu General Public Licence. Vapaiden ohjelmistojen lisenssi.
Haavoittuvuusskannaus	Verkkoskannaus käyttäen tunnettuja haavoittuvuuksia. Tarkoituksena on löytää verkon heikkoudet sen vahvistamiseksi.
Haavoittuvuustietokanta	Tietokanta, jossa on tunnettuja haavoittuvuuksia.
Hajautettu mukautuva verkkopohjaisen tunkeutumisen havaitseminen	Järjestelmä, jossa verkon osat toimivat yhteistyössä toistensa kanssa hyökkäysten havaitsemiseksi.
Havainnointikohtaiset lokitiedostot	Lokitiedostot, jotka sisältävät ainoastaan tunkeutumisen havaitsemisjärjestelmän tarvitsemat tiedot.
Hiekkalaatikko	Ympäristö, jossa ohjelmaa voidaan suorittaa rajoitetusti.
Honeyd	Matalan interaktiivisuuden hunajapurkki-ohjelmisto, jolla voidaan luoda virtuaalisia hunajapurkkeja.
Honeydsum	Honeyd-hunajapurkkien lokitiedostojen tarkasteluun tarkoitettu ohjelma.
Honeywall-palomuuri	Hunajapurkeille tarkoitettu palomuuri, joka tarkkailee ja välittää liikennettä, mutta ei estä sitä.
HTTP	Hypertext Transfer Protocol. Selainten ja www-palvelinten käyttämä tiedonsiirtoprotokolla.
Hunajapurkki	Ansa, jokna avulla kerätään hyökkäyksistä tietoa.
Hybridi	Korkean interaktiivisuuden ja matalan interaktiivisuuden hunajapurkkien tekniikoita hyödyntävä hunajapurkki.
Hyökkäysprofiili	Tunnettu toimintamalli, jota hyökkäyksen oletetaan noudattavan.
Hyökkäyskuvio	Tunnettu toimintamalli, josta hyökkäys tunnistetaan.
ICMP	Internet Control Message Protocol. Verkkokerroksen protokolla ohjausviestien lähettämiseen koneiden välillä.
IMAP	Internet Message Access Protocol. Protokolla sähköpostien lukemiseen palvelimelta.
IP	Internet Protocol. Protokolla, jonka avulla IP-paketit toimitetaan perille Internet-verkossa..

Iptables	Netfilter-palomuurin käyttöliittymä.
IRC	Intenet Relay Chat. Pikaviestintäpalvelu, jonka avulla Internet-käyttäjät voivat keskustella kirjoittamalla keskenään.
ISS-web-palvelin	Internet Information Services. Microsoftin palvelinohjelmisto Windows-laitteisiin.
Jboss IIOP/SSL	JavaBeans Open Source Software Application Server. Ohjelmistopalvelin Java-kielelle.
Keskitin	Verkkolaite, joka jakaa vastaanottamansa tietoliikenteen muuttumattomana eteenpäin.
Korkean interaktiivisuuden hunajapurkki	Hunajapurkki, jossa tunkeutujan annetaan käyttää ja asentaa ohjelmistojaan koneelle.
Laitepohjainen järjestelmä	Tarkkailee toimintaa verkon päätelaitteissa.
Lovegate-mato	Windows -järjestelmiä uhkaava mato.
MAC-osoite	Osoite, jolla verkkokortti tunnistetaan ethernet-verkossa.
Matalan interaktiivisuuden hunajapurkki	Hunajapurkki, joka jäljittelee palveluita, mutta ei anna hyökkääjien tehdä muutoksia järjestelmään.
Mentor ADSL-FR4II	Aria Technology yrityksen reititin ja palomuuri.
Microsoft EPMAP	Microsoft EndPoint Mapper. Ohjelma palveluiden etähallintaan.
Microsoft RPC DCOM	Remote Procedure Calls Distributed Component Object Model. Verkon yli hajautetun ohjelmoinnin mahdollistava ohjelmisto.
MSSQL	Microsoftin relaatiotietokantojen hallintaohjelmisto.
MySQL	Ilmainen relaatiotietokantaohjelmisto.
Nessus	Tenable Network Security yrityksen haavoittuvuusskanneri. Käytetään tietoverkkojen turvallisuuden testaukseen.
NetBIOS	Network Basic Input/Output System. Mahdollistaa tietokoneiden välisen keskustelun lähiverkon ylitse. Nimipalvelulla koneet rekisteröityvät ja istuntopalvelulla muodostetaan koneiden välinen yhteys.
Netfilter	Linux-ytimeen perustuva palomuuri.
Nmap	Verkon turvallisuusskanneri tietoverkkojen testaukseen.
Nollapäivänhyökkäys	Hyökkäys, jota ei olla vielä korjattu, mutta jota vastaan on jo olemassa hyökkäys.
Passiivinen anturi	Tietoliikennettä kuunteleva anturi.

Passiivinen järjestelmä	Järjestelmä, joka ei vaikuta kuuntelemaansa tietoliikenteeseen.
Poikkeuksien havainnointi	Normaalista toiminnasta poikkeavan tapahtuman havaitseminen.
POP3	Post Office Protocol version 3. Protokolla sähköpostien hakemiseen palvelimelta.
Porttiskannaus	Laitteen porteissa toimivien palveluiden ja ohjelmien selvityskeino.
Protokollaloukkaus	Tahallinen protokollaviestien otsakkeiden muokkaaminen vääriksi.
Ryhmälähetysviesti	Viesti, joka lähetetään yhdeltä monelle ja johon tiettyyn ryhmään kuuluneet voivat vastata.
Siltaava reititin	Reititin, joka on asetettu toimimaan läpikulkulaitteena verkkojen välillä.
Sisäinen anturi	Verkkolaitteelle asennettu anturi, jonka läpi tietoliikenne kulkee.
SMB2	Server Message Block 2. Verkkoprotokolla tiedostojen jakamiseen Microsoft Windows-tiedokoneiden välillä.
SMTP	Simple Mail Transfer Protocol. Protokolla viestien välittämiseen sähköpostipalvelimien välillä.
Snort	Avoimen lähdekoodin tunkeutumisen havaitsemisjärjestelmä.
Snort Report	Ohjelma Snort-hälytysten lukemiseen tietokannoista.
Snort-säännöt	Säännöt ohjaavat miten Snort hälyttää tietoliikenteestä.
SSH	Secure Shell. Protokolla, jolla voidaan muodostaa salattuja yhteyksiä.
Symantec pcAnywhere	Etäkäyttöohjelmisto, jolla voidaan yhdistää toisiin samaa ohjelmaa käyttäviin tietokoneisiin.
Syslog	Ohjelmisto, joka kerää lokitiedostoja ohjelmistoilta.
Systrace	Systrace on hiekkalaatikko, joka rajoittaa epäluotettujen ohjelmien pääsyä järjestelmään säätelemällä järjestelmäkutsusääntöjä.
Takaoviohjelma	Ohjelma, joka avaa järjestelmään tietoturvahaavoittuvuuden.
Tarpit	Palvelu, joka hidastaa tietoliikennettä. Tarkoituksena on kuluttaa hyökkääjän resursseja.
TCP	Transmission Control Protocol. Protokolla tietokoneiden väliseen yhteyksien luomiseen Internetin lävitse.

Tcpdump	Pakettien analysointi ohjelma, jolla voidaan tulkita tietoliikennettä.
Telnet	Verkkoprotokolla Internetin ylitse muodostettaviin pääteyhteyksiin.
Timestamp-optio	TCP-protokollan otsakkeen kenttä.
Tunkeutumisen estojärjestelmä	Järjestelmä, joka havaittuaan tunkeutujan voi tehdä toimenpiteitä hyökkäyksen etenemisen estämiseksi.
Tunkeutumisen havaitsemisjärjestelmä	Järjestelmä, joka havaittuaan hyökkäyksen kerää siitä lokitietoja ja ilmoittaa verkon ylläpitäjälle.
Tutkimushunajapurkki	Hunajapurkki, joka altistetaan täysin hyökkääjälle mahdollisimman suuren tutkimustiedon saamiseksi hyökkäyksestä.
Tuotantohunajapurkki	Hunajapurkki, jonka avulla verkkoa pyritään suojelemaan.
UDP	Use Datagram Protocol. Protokolla laitteiden väliseen yhteydettömään siirtämiseen.
Unified2	Snort-ohjelmiston ulostulotiedosto, jonne hälytykset tallentuvat binäärimuodossa.
Unix	Moniajoon kykenevä, monen käyttäjän käyttöjärjestelmä.
Vasteaika	Aika joka kuluu viestin vastaanottamisesta siihen vastaamiseen.
Verkkopohjainen tunkeutumisen havaitseminen	Tarkkailee liikennettää verkon solmukohdissa ja yrittää havaita hyökkäyksiä.
Virtuaalikone	PC-arkkitehtuuria jäljittelevä ohjelmisto.
Virtuaalipalvelin	Reitittimellä sijaitseva palvelin ohjelmisto, jonka kautta voidaan reitittää liikennettä haluttuihin portteihin.
VirtualBox	Ilmainen ohjelma käyttöjärjestelmien virtualisoimiseen.
Virtual Network Computing	Tietokoneen graafisen käyttöliittymän etäkäyttöön tarkoitettu protokolla.
Virtual Network Computer Display: 2	Tietokoneen graafisen käyttöliittymäohjelman käyttämä näyttö. Tässä numero 2.
Vulnerability Research Team	Sourcefire-tietoturvayrityksen asiantuntijaryhmä.
Waldo-tiedosto	Barnyard2-ohjelman käyttämä kirjanmerkkitiedosto.
Web-palvelin	Tietokone, joka käyttää HTTP-protokollaa sivujen jakamiseen asiakasohjelmille.
Windows Client Backup	Varmuuskopio ohjelmisto, jolla voidaan automaatisesti tehdä kopiot tiedostoista.

Xprobe	Työkalu verkossa olevan laitteen käyttöjärjestelmän tunnistamiseen.
Xsan	Storage Area Network. Applen tiedostojärjeselmä, jossa monta tietokonetta voi lukea ja muuttaa samaa tietoa samanaikaisesti.
Yleislähetysviesti	Lähetetään koko aliverkolle. Voidaan käyttää, kun halutaan saada tietoa kaikista verkossa olevista laitteista.

1 JOHDANTO

Tunkeutujaan voidaan suhtautua täydellisenä uhkana, jota vastaan on lukittava ovet ja ikkunat mahdollisimman tiukasti ja toivoa, ettei tämä löydä ullakon avonaista luukkua. Vaihtoehtoisesti tunkeutujaan voidaan suhtautua väistämättömänä pahana, jonka läsnäolosta voidaan yrittää saada suurin hyöty irti keräämällä tämän tekemisistä mahdollisimman tarkat tiedot. Näitä tiedonmuruja seuraamalla voidaan löytää verkosta aiemmin tuntemattomia haavoittuvuuksia ja heikkouksia. Hunajapurkit on suunniteltu tähän tarkoitukseen. Yhteistyössä toisten verkon havainnointityökalujen kanssa voidaan verkkoon tulevasta liikenteestä parhaimmillaan saada hyvinkin tarkka kuva.

Tällä tutkimuksella tahdottiin selvittää matalan interaktiivisuuden hunajapurkkien käyttöä verkon tarkkailussa yhdessä tunkeutumisen havaitsemisjärjestelmän kanssa. Tavoitteena oli tarkastella niiden vastaanottamaa liikennettä erilaisissa verkkorakenteissa ja arvioida saatujen tulosten perusteella hunajapurkkien hyödyllisyyttä verkon suojaamisessa yhteistyössä tunkeutumisen havaitsemisjärjestelmän kanssa.

Tietoverkot ovat jatkuvasti tietoturvahyökkäysten kohteina ja niiden suojaamiseksi kehitellään jatkuvasti uusia tekniikoita. Hyökkäyksiä verkkoihin tulee niin organisaatioden ulkopuolelta Internetistä kuin sisäpuolelta omasta sisäverkosta. Niiden havaitsemiseksi vaaditaan yhä monimuotoisempia järjestelmiä. Tässä työssä käytetään käytetään Honeyd-hunajapurkkeja ja tunkeutumisen havaitsemisjärjestelmä Snortia verkon tarkkailussa.

Testaustarkoitukseen luotiin viisi erillistä verkkorakennetta. Sijoittamalla hunajapurkkeja verkon erilaisiin kohtiin haluttiin havaita erilaista liikennettä [8]. Ensimmäisenä sisäverkkotapauksessa haluttiin jäljitellä tilannetta, jossa verkkoon oli päässyt käsiksi vihamielinen toimija. Toisena laajakaistaverkkotapauksessa haluttiin havainnoida tilannetta, jossa hyökkäys tapahtuu verkon ulkopuolelta palomuurilla suojatulle DMZ-alueelle ja sinne sijoitettuun palvelinhunajapurkkiin. Kolmantena matkapuhelinverkkotapauksessa haluttiin havainnoida matkapuhelinverkon kautta suojaamattomalle DMZ-alueelle tulevaa liikennettä ja nähdä mahdollista eroa laajakaistaverkkotapaukseen. Neljäntenä virtuaalipalvelintapauksessa haluttiin jäljitellä Internet-yhteydellisen sisäverkon tilannetta. Viidentenä hunajaverkkotapauksessa haluttiin havainnoida usean erilaisen hunajapurkin käyttöä yksittäiseen verrattuna.

Luvussa 2 käsitellään hunajapurkkiteknologiaan liittyvää teoriaa. Luvussa esitellään pääasiassa matalan interaktiivisuuden hunajapurkkeja ja niiden käyttöä verkossa. Luvussa 3 käsitellään tunkeutumisen havainnointitekniikoihin liittyvää teoriaa.

Tutustutaan siihen, miten havaitsemisjärjestelmä sijoitetaan, suojataan ja miten tunkeutuminen havainnoidaan. Luvussa 4 esitellään työssä käytetyt ohjelmistot ja tärkeimmät laitteistot. Luvussa 5 käsitellään työssä toteutetut tapaukset. Luvussa 6 esitellään ja analysoidaan tutkimuksen tulokset ja pohditaan kuinka hyvin käytetyillä ohjelmistoilla kyetään mitattu tietoliikenne esittämään sellaisessa muodossa, että se mahdollistaa tehokkaan tiedon tulkinnan.

2 HUNAJAPURKIT

Tässä luvussa tarkastellaan yleisesti hunajapurkkitekniikoita ja niihin liittyviä asioita. Erityisesti keskitytään matalan interaktiivisuuden hunajapurkkien tekniikkaan.

Tietoturvallisuuden merkitys kasvaa jatkuvasti tietoliikenteen ja verkkoon liitettävien päätelaitteiden määrän lisääntyessä. Hyökkäysten ja tietoturvallisuusuhkien tutkiminen ja liikenteen tarkoituksenmukainen vastavakoilu ovat yhä ajankohtaisempia tekniikoita. Erilaisia menetelmiä verkon suojaamiseen on monia. Esimerkiksi voidaan palomuurein ja tunkeutumisen havaitsemisjärjestelmin yrittää saada verkko tilkittyä umpeen jatkuvasti kasvavalta määrältä tunnettuja ja tuntemattomia haavoittuvuuksia. Voidaan myös pyrkiä hallittuun tietoturvauhkien ohjaamiseen pois tärkeiltä verkonlaitteilta turvallisiksi valmisteltuihin hunajapurkkikoneisiin. Niissä hyökkäystä voidaan tutkia ja kerätyn tiedon avulla voidaan verkkoa vahvistaa entisestään. [8.]

Hunajapurkkeja voidaan käyttää verkon suojaamiseen ja tietoturvahyökkäysten tutkimiseen. Hunajapurkit voidaan jakaa käyttötarkoituksiensa perusteella tuotantohunajapurkkeihin ja tutkimushunajapurkkeihin. Tuotantohunajapurkkeja käytetään hyökkäysten havaitsemiseen verkossa, niiden etenemisen hidastamiseen liikenteen tahallisella hidastamisella ja niiden ohjaamiseen tuotantojärjestelmien sijaan hunajapurkkiin. Näin hyökkääjä saadaan menemään harhaan, tuhlaamaan resurssejaan ja jättämään tutkittavissa olevaan tietoa verkon lokeihin. Tutkimushunajapurkit taas asetetaan yleensä yksikseen omaan osoiteavaruuteensa, jolloin on helppo havaita hyökkäykset, sillä kenelläkään ei pitäisi olla mitään asiaa ottaa yhteyttä hunajapurkin osoitteisiin. [8.]

Hunajapurkit voidaan vielä jakaa kahteen ryhmään sen perusteella, miten paljon ne ovat vuorovaikutuksessa hyökkääjän kanssa. Korkean interaktiivisuuden hunajapurkit pyrkivät jäljittelemään täysin oikeaa tietokonetta. Niihin luodaan vääriä tiedostoja ja hakemistoja sekä asennetaan oikeita ohjelmia ja jopa annetaan hyökkääjän tehdä muutoksia. Saadut tulokset voivat olla kattavampia, mutta myös riski järjestelmän hallinnan menettämisestä hyökkääjälle on tuntuva. Lisää korkean interaktiivisuuden hunajapurkeista Provosin ja Holzin kirjassa [1]. Matalan interaktiivisuuden hunajapurkeissa taas käytetään virtuaalisia koneita, joihin on jäljitelty oikealta vaikuttavia palveluita. Ne voivat vastata aidon tuntuisesti hyökkääjän yhteysyrityksiin, mutta eivät anna järjestelmää hyökkääjän käsiin. Hunajapurkit ja niiden yhteyteen asennetut verkonkuunteluohjelmistot, kuten tässä tutkimuksessa käytetty Snort, tallentavat hyökkääjän toiminnan lokitiedostoihin tarkasteltavaksi. [1.]

Näiden kahden ryhmän tekniikoita yhdisteleviä hunajapurkkeja kutsutaan hybrideiksi. Ne pyrkivät saamaan hyödyt molempien hunajapurkkityyppien työkaluista. Esimerkiksi voidaan aluksi käyttää korkean interaktiivisuuden hunajapurkkia uuden hyökkäyksen tutkimiseen ja ensihyökkäyksen jälkeen tulevat samankaltaiset hyökkäykset ohjataan matalan interaktiivisuuden hunajapurkkeihin tilastollisen tiedon keräämiseksi. [5.]

2.1 Matalan interaktiivisuuden hunajapurkit

Matalan interaktiivisuuden hunajapurkit jäljittelevät oikeita järjestelmiä ja niiden palveluita tai ohjelmistoja. Jäljittely tarkoittaa, että hunajapurkit sallivat hyökkääjälle rajoitetun kanssakäymisen järjestelmän kanssa ja mahdollistaa lokitiedon keräämisen hyökkäyksistä. Hunajapurkin tulisi vaikuttaa mahdollisimman todelliselta palvelulta tai koneelta hämätäkseen hyökkääjää. Huonosti toteutettu hunajapurkki saattaa aiheuttaa liikenteen katkeamisen ennen hyökkäyksen alkua taikka se voi paljastaa hunajapurkin hyökkääjälle. [5.]

Matalan interaktiivisuuden hunajapurkin hyötynä on helppous. Ne on yleensä yksinkertaisia asettaa ja ylläpitää. Tavallisesti voidaan asettaa matalan interaktiivisuuden hunajapurkki verkkoon ja jättää se keräämään tietoa. Matalan interaktiivisuuden hunajapurkeilla tavallisesti kerätään tilastollista tietoa ja korkean tason tietoa hyökkäyskuvioista. Niitä voidaan myös käyttää tunkeutumisen havaitsemisjärjestelmänä tai harhautuksena varsinaisen tuotantojärjestelmän sijasta. Matalan interaktiivisuuden hunajapurkit ovat myös turvallisempia laittaa verkkoon, sillä hyökkääjällä on rajoitetummat mahdollisuudet toimia jäljitellyn käyttöjärjestelmän kanssa. Ohjatussa järjestelmässä hyökkääjän ei pitäisi pystyä täysin saamaan sitä haltuunsa, joten ei tarvitse pelätä järjestelmän väärin käyttöä. [1; 8]

Vahvuudet ja heikkoudet

Matalan interaktiivisuuden hunajapurkeissa hyökkääjä ei kykene asentamaan tai muokkaamaan käyttöjärjestelmää. Ne sallivat ainoastaan rajoitetun pääsyn käyttöjärjestelmään. Niitä ei ole suunniteltu olemaan täysimittaisia käyttöjärjestelmiä eikä niitä siksi voi tavallisesti käyttää hyödyksi hyökkäyksissä. Tästä seuraa, etteivät matalan interaktiivisuuden hunajapurkit sovellu hyvin kaikkien hyökkäysten löytämiseen. Esimerkiksi nollapäivänhyökkäysten löytäminen vaatii monimutkaista käyttöjärjestelmän jäljittelyä. Sen sijaan sitä voidaan käyttää tunnettujen hyökkäysten havaitsemiseen ja hyökkäysten määrän mittaamiseen. Matalan interaktiivisuuden hunajapurkit tavallisesti jäljittelevät verkkopalveluja ja Internet-protokollia sen verran, että hyökkääjä erehtyy pitämää hunajapurkkia oikeana järjestelmänä. [1.]

Matalan interaktiivisuuden hunajapurkkeja on helppo asettaa ja ylläpitää. Ne eivät vaadi suurta laskentatehoa ja hyökkääjä ei voi käyttää niitä hyväksi hyökkäyksessään. Matalan interaktiivisuuden hunajapurkkien riskit ovat paljon pienemmät kuin sellaisten hunajapurkkien, joihin hyökkääjä voi murtautua ja ottaa hallintaansa. Tämä on samalla suurimpia matalan interaktiivisuuden hunajapurkkien heikkouksia. Koska hyökkääjä ei pääse toimimaan kuin jäljitellyissä palveluissa, ei voida tarkastella hyökkääjän tekniikoita silloin, kun hän on koneella. [1.]

2.2 Hunajapurkin suojaus

Tässä osiossa keskitytään lähinnä matalan interaktiivisuuden hunajapurkin suojaukseen. Näistä menetelmistä virtuaalikoneet sopivat myös korkean interaktiivisuuden hunajapurkkien suojaukseen. Niille on olemassa muitakin tarkoitukseen tehtyjä ohjelmistoja kuten hunajapurkeille tarkoitettu Honeywall-palomuuri. Näistä löytyy lisätietoa Provosin ja Holzin kirjasta [1].

Hyökkääjä ei voi täysin ottaa matalan interaktiivisuuden hunajapurkkia hallintaansa. Tämä tekee sen suojaamisesta helpompaa, koska sillä on vähemmän uhkia, joihin pitää valmistautua. Esimerkiksi jäljitellyt palvelut eivät yleensä anna hyökkääjän asentaa työkaluja ja suorittaa palvelunestohyökkäyksiä hunajapurkkikoneelta käsin. [1.]

Hunajapurkissa voi kuitenkin olla haavoittuvuuksia ja virheitä, jolloin hyökkääjä voi onnistua murtamaan sen. Siksi on hyvä varautua käyttämällä hunajapurkkia suojatussa tai rajatussa ympäristössä. Tällöin järjestelmä on edelleen suojassa vihamieliseltä käyttäjältä.

Suojaukseen voidaan käyttää Chroot Jail-ohjelmaa, Systrace-ohjelmaa, virtuaalikoneita tai iptables-palomuuria. Chroot Jail- ja Systrace-ohjelmilla hunajapurkin toiminta voidaan rajata pienelle alueelle järjestelmää. Virtuaalikoneilla voidaan hunajapurkki asettaa virtuaaliympäristöön. Iptables-palomuurilla voidaan suojata hunajapurkkia ajava järjestelmä taikka voidaan hunajapurkille saapuvasta liikenteestä sallia vain haluttu osa.

Chroot Jail

Chroot-komennolla voidaan rajoittaa ohjelma pienelle alueelle tiedostojärjestelmää. Tämä tehdään muuttamalla ohjelman tiedostojärjestelmänjuuri johonkin tiettyyn hakemistoon. Tämän jälkeen ohjelma ei voi enää käyttää mitään muita tiedostoja kuin niitä, jotka sijaitsevat siinä hakemistossa. Tällöin vaikka hyökkääjä pääsisikin käsiksi kyseessä olevaan ohjelmaan, hän ei näe mitään muuta kuin hakemistossa olevat tiedostot. Hunajapurkki ja sen kaikki tarpeelliset tiedostot on siis asennettava rajoitettuun tiedostojärjestelmän osaan, jotta se saadaan toimimaan sillä alueella. [1.]

Matalan interaktiivisuuden hunajapurkkia ei kannata käyttää pääkäyttäjänä. Pääkäyttäjän oikeuksilla on monta keinoa murtautua pois Chroot Jail-alueelta. Hunajapurkin käyttämiseen kannattaa käyttää sellaisia käyttäjätunnuksia, joita kukaan muu ei käytä. Chroot ei ole täydellinen. Voidaan käyttää hyväksi Unix-järjestelmien heikkouksia järjestelmän ottamiseksi hallintaan. Se kuitenkin toimii yhtenä lisäsuojana järjestelmälle [1.]

Systrace

Toinen tapa suojata hunajapurkkia on käyttää Systrace-ohjelmistoa. Systrace on hiekkalaatikko, joka on saatavilla monelle Unix-järjestelmälle. Se rajoittaa epäluotettujen ohjelmien pääsyä järjestelmään säätelemällä järjestelmäkutsusääntöjä. Hiekkalaatikko tarkastaa järjestelmäkutsun ja sen parametrit, ennen kuin se sallii sen ajamisen. Voidaan esimerkiksi sallia vain hunajapurkin tarvitsemien tiedostojen käyttämisen ja estää muiden tiedostojen käyttö kokonaan. [1.]

Jotta voidaan käyttää Systrace-ohjelmaa hunajapurkin kanssa, on luotava käytäntöjä, jotka ovat erityisesti siihen tarkoitukseen luotuja. Systrace-ohjelma osaa tarvittaessa oppia käytännöt interaktiivisesti. Systrace hälyttää aina, kun jokin ohjelma yrittää suorittaa toimintoa, jota ei ole nykyisessä käytännössä sallittu, jolloin sitä voidaan muokata tarpeen mukaan. Systrace-ohjelma tallentaa hälytykset syslog-lokitiedostoon. [1.]

Virtuaalikone

Kolmas keino suojata hunajapurkkia on käyttää virtualisointia. Hunajapurkki voidaan luoda virtuaalikoneelle, joka jäljittelee pc-arkkitehtuurin konetta. Sille asennetaan jäljiteltävä käyttöjärjestelmä aivan kuten fyysiseen tietokoneeseen. Virtuaalikone saadaan asetettua siltaavaan tilaan, jolloin se vaikuttaa verkossa erilliseltä tietokoneelta. [1. s. 22]

Hunajapurkki-ohjelmisto ja sen tarvitsemat tiedostot asennetaan virtuaalikoneelle. Tarvittaessa se toimii eristettynä alueena hunajapurkille. Näin saadaan suojattua virtuaalikonetta ajava isäntäkone, sillä mahdollinen hyökkäys tapahtuu virtuaalikoneen sisällä. Kuitenkin, jos virtuaalikoneessa on virheitä tai haavoittuvuuksia se voi heikentää järjestelmän tietoturvallisuutta. [8.]

Virtualisointi tuo monia mahdollisuuksia käytettäväksi. Virtuaalikone voidaan helposti varmuuskopioida, se voidaan siirtää fyysisestä laiteesta toiseen tiedostona ja jos virtuaalikoneen turvallisuus on vaarantunut tavalla, jolla sen ei ollut tarkoitus, se voidaan helposti poistaa, taikka tallentaa myöhempää tarkastelua varten. [10. s. 228]

Iptables

Iptables on Netfilter palomuuriohjelman käyttöliittymä. Se tarkastelee ja ohjaa pakettiliikennettä. Jatkossa niitä kutsutaan pelkällä Iptables-nimityksellä. Tarkemmin sanoen se tarkastelee tietoliikennepaketteja ja suodattaa niitä tarpeen mukaan. Sille määritellään säännöt, joiden perusteella se torjuu, päästää ja uudelleen ohjaa saapuvaa tietoliikennettä. [8. s. 311]

Palomuurilla voidaan suojata hunajapurkkia ajavaa järjestelmää. Esimerkiksi Honeyd-ohjelmisto luo käyttöjärjestelmään virtuaalisia hunajapurkkeja. Tällöin on hyvä suojata järjesteltelmä turhalta liikenteeltä. Asetetaan Iptables päästämään ainoastaan hunajapurkkien osoitteisiin saapuva liikenne esteettömästi ja estetään käyttöjärjestelmän osoitteeseen tuleva liikenne kokonaan.

2.3 Hunajapurkilla houkuttelu

Hunajapurkit houkuttelevat hyökkääjiä paljastamalla tarkoituksella erilaisia tunnettuja haavoittuvuuksia. Hyökkäyksen aikana voidaan ottaa talteen hyökkääjän toiminnot, jotta voidaan saada selville hänen toimintansa ja tekniikkansa. Hyökkäyksiä tutkimalla voidaan vahvistaa omien järjestelmien turvallisuutta.

Hunajapurkilla pitäisi olla tavallisimmat palvelut käytössä, jotta se vaikuttaa aidolta koneelta. Näitä ovat esimerkiksi telnet-palvelin (portti 23), HTTP-palvelin (portti 80) ja FTP-palvelin (portti 21). Siinä missä korkean interaktiivisuuden hunajapurkeilla nämä palvelut ovat käytössä, matalan interaktiivisuuden hunajapurkeilla niitä jäljitellään erilaisin ohjelmin. Hunajapurkin pitäisi sijaita jossakin oikean palvelimen lähellä, jotta hyökkääjät luulevat helpommin sen olevan varsinainen palvelin, esimerkiksi vierekkäisessä IP-osoitteessa. Voidaan myös asettaa palomuuri tai reititin reitittämään tiettyjen porttien liikenne hunajapurkille, jossa hyökkääjä uskoo yhdistävänsä oikeaan palvelimeen. Kannattaa asettaa hälytykset siten, että heti kun hunajapurkkiin tulee hyökkäys siitä ilmoitetaan ylläpitäjälle. Kannattaa myös pitää lokitiedostot toisella koneella, jotta hyökkääjä ei pysty tuhoamaan niitä siinä vaiheessa, kun hunajapurkki on hyökkäyksen alaisena. [3.]

Hunajapurkin pitää näyttää oikealta järjestelmältä. Korkean interaktiivisuuden hunajapurkkiin on luotava vääriä tiedostoja, käyttäjätilejä ja niin edelleen. Matalan interaktiivisuuden hunajapurkkeihin on taas luotava palveluita ja toiminnallisuutta, jotta voidaan varmistaa, että hyökkääjä uskoo sen olevan oikea järjestelmä. Tällöin hyökkääjä jää järjestelmään pidemmäksi aikaa. [8.]

2.4 Hunajapurkin havaitseminen

Jotta hunajapurkki voidaan naamioida on tiedettävä, miten hunajapurkkeja voidaan havaita. Tässä keskitytään lähinnä matalan interaktiivisuuden hunajapurkkien havaitsemiseen. Korkean interaktiivisuuden hunajapurkkien havaitsemisesta voi lukea lisää Provosin ja Holzin kirjasta [1. s.280]. Hunajapurkin realistisuus on tärkeää. Mitä realistisempi hunajapurkki sitä paremmin se harhauttaa hyökkäyksen tekijää. Tällöin saadaan kerättyä enemmän tietoa, koska hyökkäyksistä tulee pidempiä ja hyökkääjien toimista monipuolisempia. [1.]

Hunajapurkin paljastuessa hyökkääjälle tämä voi yrittää peitellä jälkiänsä tai jättää hunajapurkin täysin koskemattomaksi. Mikäli hyökkääjä onnistuu saamaan hunajapurkin huomaamatta hallintaansa, voi hän käyttää sitä hyödyksi verkkohyökkäyksien suorittamisessa. [1.]

Matalan interaktiivisuuden hunajapurkille on tärkeää pystyä hämäämään verkonskannaustyökaluja. Varsinkin virtuaalikoneilla pyörivän hunajapurkin on vaikea pysyä huomaamattomana. Ne eivät esitä kokonaista käyttöjärjestelmää hyökkääjille, vaan jäljittelevät sen palveluita. Siksi voidaan päätellä, että koska niihin ei voida murtautua eivätkä ne tarjoa monimutkaisia palveluja, ne saattavat olla hunajapurkkeja. On myös mahdollista, että jäljitellään epärealistisia yhdistelmiä, kuten Windows Web-palvelin ja Unix FTP-palvelin samassa hunajapurkissa. [1.]

Matalan interaktiivisuuden hunajapurkkeihin ollaan kosketuksissa verkon välityksellä. Käytännössä on olemassa fyysinen kone, jolla hunajapurkki on käynnissä. Tämän koneen resurssit ovat jaettuna käyttöjärjestelmän ja hunajapurkin kanssa. Jos löytyisi keino hidastaa käyttöjärjestelmää, huomattaisiin että myös hunajapurkki alkaa hidastua tai sen vasteajat ovat pidempiä kuin aiemmin. Esimerkiksi, jos samalla koneella hunajapurkin lisäksi sijaitsee web-palvelin, voitaisiin sille lähetetyillä HTTP-pyynnöillä hidastaa matalan interaktiivisuuden hunajapurkkeja. [1.]

Hunajaverkko voidaan myös paljastaa kuormittamalla niistä yhtä ja havaitsemalla hidastuminen ja vasteaikojen kasvaminen muissa hunajaverkon purkeissa. Kaikilla samalla koneella sijaitsevilla hunajapurkeilla on muitakin yhtenäisiä ominaisuuksia, joita tarkkailemalla voidaan päätellä tiettyjen koneiden olevan hunajapurkkeja. Esimerkiksi voidaan tarkkailla TCP-protokollan Timestamp-optiota. Ajan myötä järjestelmän kellonaikaan tulee vääristymää ja kaikki samalla koneella olevat hunajapurkit jakavat saman suuruisen vääristymän. Tätä vastaan on joissain hunajapurkeissa ryhdytty tarjoamaan jokaiselle purkille oma vääristymänsä. [1. s. 276]

Toisenlainen lähestymistapa on tutkia matalan interaktiivisuuden hunajapurkkien verkkovastauksia ja etsiä poikkeavia tietoja ja käyttäytymistä. Tämän voi tehdä hyväksi käyttämällä hunajapurkeissa olevia korjaamattomia vikoja ja tunnettua toimintaa.

Esimerkiksi tarpit-tekniikka, jolla tietoliikennettä hidastetaan hyökkääjän ajan ja resurssien kuluttamiseksi, voidaan havaita tutkimalla tcpdump-tulostetta. Tcpdump on tietoliikennepakettien analysointityökalu. Havaitaan, että tarpit on toteutettu käyttäen harvoin käytettyjä TCP tekniikoita. [1.]

Virtuaalikoneita ei ole suunniteltu olemaan läpinäkyviä. Niiden tarkoituksena on virtualisoida tietokone eikä piilottaa sitä, että kyseessä on virtuaalikone. Jos hyökkääjä pääsee virtuaalikoneelle, hän voi kohtalaisen helposti saada sen paljastettua. Esimerkiksi kehittäjällä voi olla tapana nimetä verkkoliitännöiden MAC-osoitteet aina saman merkkiyhdistelmän mukaisesti. Tällöin niistä voidaan päätellä, että kyseessä on virtuaalikone. Nämä ovat korkean interaktiivisuuden hunajapurkeille ongelma, ja niiden peittämiseen on saatavilla työkaluja ja päivityksiä. Matalan interaktiivisuuden hunajapurkkien kohdalla hyökkääjillä ei ole pääsyä käsiksi laitteistoon, mutta verkkoliikenteestä voidaan päätellä esimerkiksi, että saman MAC-osoitteen omaavat laitteet voivat olla virtuaalikoneessa. [1. s. 292]

Tässä esiteltiin vain muutamia matalan interaktiivisuuden hunajapurkkien havaitsemistapoja. Hyökkääjät etsivät jatkuvasti uusia heikkouksia ja tapoja hunajapurkkien löytämiseen ja häiritsemiseen. Voi olla vain ajan kysymys kuinka pitkään hunajapurkki saa olla verkossa ennen kuin, joku on sen havainnut ja lisännyt löydettyjen hunajapurkkien listalle verkon hämäräperäisemmille sivustoille. Sen jälkeen hyökkäykset voivat loppua kokonaan, olla paljon suunnitelmallisempia, taikka niiden tarkoituksena voi olla vain hunajapurkin häiritseminen loputtomalla liikenteen tulvalla.

2.5 Hunajapurkin asemointi verkkoon

Hunajapurkkeja voidaan sijoittaa useisiin erilaisiin paikkoihin. Paikan valinta vaikuttaa siihen, minkälaista liikennettä sille saapuu. Paikan valinta riippuu siitä, minkälaista tietoa ja käyttöä hunajapurkilta tahdotaan, sekä kuinka suurta riskiä ollaan valmiita sietämään sen keräämiseksi. [8.]

Verkon eri osilla voidaan sanoa olevan erilainen turvallisuuden taso. Esimerkiksi DMZ-alueelle on sallittu paljon vapaammin liikennettä, kuin sisäverkolle. Turvallisuuden tason määrittely riippuu siitä, mitä verkon siinä osassa sijaitsee. Sellaiseen verkon osaan, jossa ei sijaitse web-palvelinta, ei tarvitse päästää porttiin 80 kulkevaa liikennettä ja sellaisen liikenteen saapuminen aiheuttaisi hälytyksen tunkeutumisen estojärjestelmissä. [3.]

Sijoittamalla hunajapurkki ulkoisen palomuurin ulkopuolelle voidaan seurata verkon käyttämättömiin IP-osoitteisiin tulevia yhteysyrityksiä. Näin sijoitettu hunajapurkki ei aiheuta vaaraa sisäverkon koneille. Lisäksi tämä sijoitus vähentää verkon hallintaohjelmien aiheuttamia hälytyksiä. Heikkoutena tällä sijoituksella on, ettei se kykene havaitsemaan verkon sisäisiä hyökkääjiä. [8.]

Toinen paikka sijoittaa hunajapurkki on DMZ-alueelle. Silloin muut sinne sijoitetut laitteet on syytä suojata siltä varalta, että hunajapurkki onnistutaan murtamaan. Heikkoutena on, että tavallisesti DMZ-alue ei ole täysin avoin vaan palomuuri torjuu myös sille saapuvaa liikennettä. On siis heikennettävä palomuurin DMZ-sääntöjä taikka hyväksyttävä rajoitettu hunajapurkin tehokkuus. [8.]

Kolmas sijainti paikka on sisäverkossa. Sen tärkein etu on siinä, että se voi havaita verkon sisäisiä hyökkäyksiä. Sisäverkon hunajapurkki kykenee myös havaitsemaan väärin asetetun palomuurin, joka ohjaa väärää liikennettä Internetistä sisäverkkoon. Suurin heikkous on siinä, että jos hunajapurkki onnistutaan murtamaan, sitä voidaan käyttää hyökkäyksissä toisiin verkon laitteisiin. Palomuuri ei estäisi liikennettä, sillä se on hunajapurkille suuntautuvaa ja siksi sallittua liikennettä. Myös tässä sijainnissa on joko muutettava palomuurin asetuksia sallimaan hunajapurkille tulevaa liikennettä tai on hyväksyttävä hunajapurkin pienempi tehokkuus. [8.]

Tämän tutkimuksen tapauksissa hunajapurkit on sijoitettu mukaillen edellä mainittuja sijainteja. Sisäverkkotapauksessa hunajapurkki on osana sisäverkkoa. Matkapuhelinverkkotapauksessa hunajapurkki on asetettu osaksi ulkoverkkoa sijoittamalla se DMZ-alueelle siten, että palomuuri on kokonaan poissa päältä. Laajakaistaverkkotapauksessa hunajapurkki on DMZ-alueella, mutta palomuuri on edelleen päällä. Hunajaverkkotapauksessa toteutettiin neljän hunajapurkin verkko, joiden palveluihin ohjattiin liikennettä.

3 TUNKEUTUMISEN HAVAITSEMINEN

Tässä luvussa keskitytään pääosin verkkoa kuuntelevien havainnointijärjestelmien toimintaan. Lisäksi on olemassa yksittäisten isäntäkoneiden tarkkailuun perustuvia laitepohjaisia järjestelmiä.

Tietokoneverkkojen turvallisuuden keskeisenä osana on hyökkäysten havaitseminen ja niihin reagointi. Tunkeutumisen havaitsemis- ja estämisjärjestelmät toimivat verkon valvojina. Ne tallentavat epäilyttävät tapahtumat liikenteen lokitiedostoihin ja hälyttävät verkon ylläpitäjälle, kun tapahtumat täyttävät ennalta määritellyt säännöt tapahtumista. Ohjelmistot, kuten Snort ja sen liitännäiset, auttavat tietoliikenneuhkien havaitsemisessa, analysoinnissa ja hyökkäysten alkuperän jäljittämisessä. Sääntöinä toimii joukko valmiiksi tunnettuja hyökkäyskuvioita. Valmiiden sääntöjen lisäksi säännöt voidaan luoda itse omiin tarkoituksiin sopiviksi.

Hunajapurkit toimivat liikenteen havaitsemisessa tehokkaasti, koska niille tuleva liikenne on poikkeuksetta verkkoon kuulumatonta. Tunkeutumisen havaitsemis- ja estämisjärjestelmät yhdessä hunajapurkkiohjelmistojen kanssa muodostavat verkosta paremmin hallittavan ja valvottavan kokonaisuuden. Sen avulla voidaan estää tietoturvahyökkäyksiä ohjaamalla ne pois avainkohteista ja vahvistaa verkon tietoturvaa niistä kerättyjen tietojen perusteella.

Tässä tutkimuksessa on käytetty Snort-ohjelmistoa, joka on hyökkäyksen havaitsemisjärjestelmä. Se pyrkii havaitsemaan ja hälyttämään hyökkäyksen tapahtuessa. Snort on passivinen järjestelmä ja sen aseita ovat hyökkäyksien havainnointi, hälytysten antaminen näytölle ja tietojen välittäminen niitä keräävälle ohjelmille.

Hyökkäyksen estämisjärjestelmät puolestaan ovat aktiivisempia ja aggressiivisempia toimimaan, kun mahdollinen hyökkäys havaitaan. Havaitsemisen, lokien luomisen ja hälytyksen antamisen lisäksi epäilyttävä verkkoliikenne voidaan esimerkiksi estää ja yhteyksiä voidaan katkaista. Tutkimuksessa valittiin käyttöön passiivinen järjestelmä, koska se sopii hyökkäystiedon keräämiseen yhteistyössä samassa verkossa toimivien hunajapurkkien kanssa. Passiivinen järjestelmä päästää epäilyttävän liikenteen kulkemaan hunajapurkkien ja ulkoverkon välillä, jolloin liikenteestä saadaan kerättyä lokitiedostoja koko yhteyden ajalta.

3.1 Hyökkäyksen tunnistus

Tunkeutumisen havaitsemiseminen perustuu siihen, että tunkeilijan toiminta eroaa jotenkin luvallisen käyttäjän toiminnasta. Kuitenkin osa tunkeilijan toimista ovat muiden käyttäjien kanssa yhteneviä ja jää siksi havaitsematta. Liian väljillä tunkeilijan määrittelyillä saadaan paljon vääriä tuloksia ja liian tiukoilla määrittelyillä havaitsematta jääneiden tunkeilijoiden määrä kasvaa. On pyrittävä löytämään keskitie. Tunkeutumisen havaitsemisjärjestelmissä tätä päällekkäisyyttä oletetaan tapahtuvan ja sitä on pyritty ottamaan huomioon niitä suunnitellessa. [8.]

Tunkeilijat

Verkon tunkeilijat voidaan jakaa naamioitujiin, oikeuksiensa väärinkäyttäjiin ja luvattomiin käyttäjiin. Naamioituja tunkeutuu järjestelmään pyrkimyksenä hyväksikäyttää oikeiden käyttäjien käyttäjätilejä. Naamioituja on todennäköisesti ulkopuolinen hyökkääjä. Oikeuksien väärinkäyttäjä käyttää ohjelmia ja resursseja, ja katselee tietoa, johon hänellä ei ole lupaa päästä käsiksi taikka hän käyttää väärin lupaansa. Useimmiten kyseessä on sisäinen uhka. Luvaton käyttäjä ottaa järjestelmän haltuunsa ja käyttää sitä tarkastusten ja pääsynhallinnan ohittamiseen. Kyseessä voi olla sisäinen tai ulkoinen uhkatekijä. [8.]

Verkkopohjainen tunkeutumisen havaitseminen

Verkkopohjaiset tunkeutumisen havaitsemisjärjestelmät tarkkailevat liikennettä verkkojen solmukohdissa. Ne tarkastelevat solmukohdan läpi kulkevaa liikennettä hyökkäyskuvioiden havaitsemiseksi. Ne käyttävät hyödykseen poikkeuksien ja allekirjoitusten havaitsemista. Siinä missä laitepohjainen järjestelmä tarkastelee käyttäjien ja ohjelmistojen toimintaa, verkkopohjainen järjestelmä tarkastelee verkon laitteille suunnattua pakettiliikennettä. Verkkopohjainen tunkeutumisen havaitsemisjärjestelmä koostuu antureista, jotka tarkkailevat pakettiliikennettä, havaitsemisjärjestelmän hallintaan tarkoitetuista palvelimista ja hallintaan tarkoitetuista päätelaitteista. [8.]

Anturit voivat olla sisäisiä tai passiivisia tai niiden yhdistelmiä. Sisäinen anturi on sijoitettu verkkoon siten, että sen tarkkailema liikenne kulkee sen läpi. Se voidaan sijoittaa verkkolaitteelle, kuten palomuuriin tai kytkimeen. Ei siis vättämättä tarvita ylimääräistä laitetta verkkoon vaan voidaan käyttää verkossa jo olevia laitteita. Sisäisten anturien käyttötarkoitus on auttaa hyökkäysten pysäyttämisessä, kun sellainen havaitaan. Toisin kuin sisäisissä antureissa, passiivisissa antureissa liikenne ei kulje sen

läpi. Sen sijaan sille kulkeutuu verkon liikennettä kuten muillekin verkon koneille. Passivisen anturin etuna on, ettei se hidasta verkkoliikennettä. [8.]

Hajautettu mukautuva verkkopohjainen tunkeutumisen havaitseminen

Hajautettu verkkopohjainen tunkeutumisen havaitsemisjärjestelmä tarkkailee verkon tapahtumia ja verkkolaitteita. Voidaan käyttää yhtä keskitettyä tunkeutumisen havaitsemisjärjestelmää hallinnoimaan ja ohjaamaan hallinnoitavien verkkojen paikallisia järjestelmiä. Stallingsin mukaan viime vuosina keskenään kommunikoivat tunkeutumisen havaitsemisjärjestelmät ovat kehittyneet pitämään sisällään hajautettuja järjestelmiä, jotka tekevät yhteystyötä tunkeutumisien havaitsemiseksi ja muuttuviin hyökkäysprofiileihin mukautumiseksi. [8.]

Yksittäiset tietoturvajärjestelmät ovat aina kärsineet siitä, etteivät ne välttämättä pysty tunnistamaan uusimpia hyökkäyksiä ja siitä, että on ollut hankalaa päivittää nopeasti niiden toimintamallia vastaamaan nopeasti leviäviin hyökkäyksiin. Uudempi ja vaikeammin havaittavissa oleva hyökkäystyyppi on hitaasti levittäytyvät hyökkäykset. Sellaisten hyökkäysten torjumiseksi on käytettävä yhteistyössä toimivia järjestelmiä, jotka havaitsevat hyökkäyksen pienistä verkon koneilta kerätyistä vihjeistä. Kun mukautuvassa yhteistyössä toimivassa järjestelmässä jokin verkon laitteista epäilee mahdollisen hyökkäyksen olevan käynnissä, se ilmoittaa epäilyksestään muille laitteille. Verkon laiteet odottavat, kunnes saavat raja-arvon ylittävän määrän viestejä, ennen kuin ne tekevät uhkaan liittyviä toimenpiteitä ja lähettävät hälytyksen hallintajärjestelmälle. [8.]

Laitepohjainen tunkeutumisen havaitseminen

Laitepohjaiset tunkeutumisen havaitsemisjärjestelmät lisäävät tärkeiden järjestelmien tietoturvallisuutta. Niillä tarkastellaan järjestelmä epäilyttävän toiminnan varalta ja niitä voidaan välillä käyttää hyökkäysten kulun pysäyttämiseen. Niiden päätarkoitus on kuitenkin havaita hyökkäykset, kerätä niistä lokitiedostot ja lähettää järjestelmän hallitsijalle hälytys. Laitepohjaisten tunkeutumisen havaitsemisjärjestelmien etuna verrattuna verkkopohjaisiin järjestelmiin on, että niillä voidaan havaita niin sisäiset kuin ulkoiset hyökkäykset. [8.]

Kuten verkkopohjaiset tunkeutumisen havaitsemisjärjestelmät, myös laitepohjaiset järjestelmät tunnistavat hyökkäyksiä kahdella eri tekniikalla. Laitepohjainen tunkeutumisen havainnointi pystyy poikkeuksien havainnoinnilla löytämään sellaisia tunkeutujia, jotka eivät pyri jäljittelemään tavallisten käyttäjien toimia, mutta ei välttämättä onnistuta löytämään oikeuksiensa väärinkäyttäjiä. Allekirjoitusten

havaitsemistekniikoilla saatetaan tilanteeseen liittyvistä tapahtumista tunnistaa tunkeutuminen. [8.]

Hajautettu laitepohjainen tunkeutumisen havaitseminen

Laitepohjaisia tunkeutumisen havaitsemisjärjestelmiä voidaan käyttää myös hajautetusti sisäverkon laitteilla. Verkon eri osiin sijoitetut tunkeutumisen havaitsemisjärjestelmät asetetaan toimimaan yhteistyössä keskenään tehokkaan puolustuksen saavuttamiseksi. Verkossa voi olla yksi tai useampi laite, riippuen verkon rakenteesta, jolle muut laitteet lähettävät lokitietonsa. Tarkkailtavana voi olla useita paikallisverkkoja ja niistä jokaisella voi olla oma keskuslaitteensa, joka sitten lähettää keräämänsä tiedot eteenpäin kaikkia verkkoja hallinnoivalle tunkeutumisen havaitsemisjärjestelmälle. [8.]

Allekirjoituksen ja poikkeuksen havaitseminen

Allekirjoituksien havaitsemisessa järjestelmä tarkastelee liikennettä verkossa käyttäen sääntöjä, joiden perusteella se määrittelee onko tietty kuvio liikenteessä epäilyttävä. Verkkoliikenteestä tarkkaillaan protokollien hyväksikäyttöön liittyviä kuvioita, verkkoskannauksia, väärennettyjä IP-osoitteita ja odottamattomien ohjelmistojen palveluita. [8.]

Poikkeuksien havainnoinnissa käytetään pääasiassa raja-arvon tarkastelua ja profiilien tarkastelua. Raja-arvoa tarkastellessa lasketaan tietyn tyyppisen tapahtuman määrä jollakin ajanjaksolla. Mikäli määrä ylittää sopivaksi määritellyn määrän annetaan siitä hälytys. Profiileihin perustuvassa poikkeuksien havaitsemisessa pyritään tarkkailemaan verkon normaalia liikennettä ja vertaamaan uutta liikennettä siihen. Mikäli liikenteessä on suuria muutoksia, oletetaan että kyseessä voi olla tunkeilija. Poikkeuksien havainnoinnilla voidaan havaita esimerkiksi palvelunestohyökkäyksiä, verkkoskannauksia ja matoja. [8.]

3.2 Sijoittaminen verkkoon

Tunkeutumisen havaitsemis- ja estojärjestelmät voidaan haluta asettaa yhteen tai useampaan paikkaan. Sijainnin valinta riippuu verkon rakenteesta sekä siitä, minkä tyyppisiä tunkeutumisyrityksiä halutaan havaita. [3.]

Jos halutaan havaita ulkoisia tunkeutumistoimia, paras paikka tunkeutumisen havaitsemisjärjestelmälle voi olla ulospäin suuntautuvan reitittimen sisällä taikka palomuurissa. Tällöin se kykenee havaitsemaan hyökkäyksiä, jotka saapuvat ulkoverkosta. Vaikka kaikkia tulevia hyökkäyksiä ei kyettäisikään havaitsemaan,

saatetaan joskus huomata sisäverkosta tuleva epäilyttävä liikenne. Jos verkossa on useita reittejä Internetiin, voi olla hyvä laittaa anturi jokaiseen sisääntuloon. [3; 8]

Tunkeutumisen havaitsemisjärjestelmän anturi voidaan myös asettaa ulkoisen palomuurin ja Internetin välille. Tällöin on mahdollista tarkkailla täysin suodattamatonta liikennettä ja kerätä tietoa verkkoon suuntautuvien hyökkäysten määrästä ja laadusta. [8.]

Anturi voidaan myös asettaa suurimpien liikennekanavien varrelle. Tällöin saadaan kerättyä mahdollisimman suuri määrä tietoa liikenteestä ja kasvatetaan hyökkäyksen havaitsemisen todennäköisyyttä. Tämä sijoitus myös helpottaa verkossa tapahtuvan luvattoman toiminnan havaitsemisessa. [8.]

Sisäisten uhkien havaitsemiseksi antureita on asetettava jokaiseen verkon osaan. Hunajapurkit ovat tehokkaita sisäisten uhkien havaitsemisessa ja niitä voidaan käyttää osana verkon havaitsemisjärjestelmää. Tavallisesti sisäverkon koneet eivät yritä lähettää liikennettä hunajapurkkikoneelle, joten kaikki sille kohdistuva verkon skannaus tai muu liikenne on epäilyksen alaista. [8.]

Jos verkossa on DMZ-alue, tunkeutumisen havaitsemisjärjestelmä voidaan myös sijoittaa sinne. Hälytyskäytäntöjen ei kuitenkaan pitäisi olla yhtä tiukkoja kuin verkon yksityisissä osissa. [3.]

Parhaimmassa tapauksessa tunkeutumisen havaitsemis- ja estojärjestelmänantureita on asennettu jokaiseen verkon osaan. Koska resurssit ovat kuitenkin rajalliset kannattaa keskittyä tärkeimpien osien tarkkailemiseen. [3; 8]

3.3 Tunkeutumisen havaitsemisjärjestelmän suojaus

Tässä keskitytään pääosin tutkimuksessa käytetyn tunkeutumisen havaitsemisjärjestelmä Snortin suojaamiseen. Tarkemmin voi lukea Rehmanin kirjasta [3.]. On tärkeää suojata tunkeutumisen havaitsemisjärjestelmä. Jos se vaarantuu voidaan saada vääriä hälytyksiä tai hälytyksiä ei tule ollenkaan. Tunkeilija voi sammuttaa tunkeutumisen havaitsemisjärjestelmän, ennen kuin tekee varsinaisen hyökkäyksen. On olemassa monia erilaisia tapoja suojata järjestelmä, joista tässä esitellään muutama. [3.]

Tässä tutkimuksesta asetettiin Snort-ohjelma kuuntelemaan verkkoliitäntää, jolle ei ole ollenkaan asetettu IP-osoitetta. Esimerkiksi Linux-koneella voidaan nostaa ethernetliitäntä päälle yksinkertaisella komennolla ilman, että sille asetetaan varsinaista IP-osoitetta. Etuna on, että kun Snort-isännällä ei ole IP-osoitetta, kukaan ei voi ottaa siihen yhteyttä. Laitteen toiselle verkkoliitännälle voidaan asettaa IP-osoite, johon ylläpitotyöasema voitaisiin kytkeä. [3.]

Tunkeutumisen havaitsemisjärjestelmän anturissa ei kannata ajaa mitään palveluita. Verkkopalvelimet ovat yksi yleisimmistä tavoista hyväksikäyttää järjestelmiä. Käytettävien järjestelmien pitäisi olla päivitetty kaikkein uusimpiin ohjelmistoihin ja

päivityksiin. Tunkeutumisen havaitsemisjärjestelmä kannattaa asettaa siten, ettei se vastaa ICMP-viesteihin. Tunkeutumisen havaitsemisjärjestelmää ei pidä käyttää mihinkään muuhun kuin tunkeutumisen havaitsemiseen, eikä sille pidä luoda muita käyttäjätilejä kuin välttämättömät. [3.]

Linux-järjestelmissä voidaan käyttää iptables-palomuuria estämään ei haluttu liikenne. Snort kykenee silti edelleen näkemään kaiken tietoliikenteen. Tässä tutkimuksessa käytettiin iptables-palomuuria suojaamaan hunajapurkkia ja virtuaalikonetta ajavia järjestelmiä. [3.]

Snort voidaan myös asettaa hiljaiseen tilaan, joka ainoastaan kuuntelee saapuvaa liikennettä, muttei lähetä mitään paketteja ulos. Tämä on siis saman kaltainen kuin yllä mainittu liitäntä ilman IP-osoitetta. Hiljaiseen verkkoliitäntään käytetään erityistä kaapelia, jossa Snort-koneen päässä on johdon pinnit 1 ja 2 oikosuljettu. Pinnit 3 ja 6 on yhdistetty samoihin pinneihin kaapelin toisessa päässä sijaitsevaan kuunneltavaan verkkolaitteeseen. [3.]

3.4 Tietoliikenteen uhkan arviointi

Tässä tutustutaan lyhyesti tietoliikenteen arviointiin. Pyritään löytämään viitteitä epäilyttävästä liikenteestä verkon laitteiden tallentamasta lokitiedosta ja tapahtumista. Etsitään tietoja sellaisten palveluiden ja protokollien käytöstä, jotka viittaavat laitteen turvallisuuden vaarantuneen. Tämän kaltainen tarkastelu on tärkeä lisä tunkeutumisen havaitsemisjärjestelmän tueksi. Verkossa olevilta hunajapurkeilta saadaan hyödyllistä lokitietoa tarkastelun avuksi. Tämä voi olla työlästä ja aikaa vievää työtä. Esimerkiksi tässä tutkimuksessa käytettiin Honeyd-hunajapurkkiohjelmiston lokitiedostojen tarkkailuun Honeydsum-ohjelmistoa. [2.]

Lisäksi kerättyä tietoa syötetään tunkeutumisen havaitsemisjärjestelmille. Kaksi tapaa kerätä havaitsemisjärjestelmälle syötettävää tietoa ovat alkuperäiset lokitiedostot ja havainnointikohtaiset lokitiedostot. Alkuperäiset lokitiedostot ovat laitteiden ja ohjelmistojen järjestelmälokeja. Näiden käytön etuna on ettei niiden keräykseen tarvitse käyttää erillistä ohjelmaa. Havainnointikohtaisia lokitiedostoja saadaan käyttämällä ohjelmaa, joka tuottaa ainoastaan tunkeutumisen havaitsemisjärjestelmän tarvitsemia tietoja. Tällä ratkaisulla voidaan tuottaa mille tahansa järjestelmälle sopivia tietoja, joten ei olla riippuvaisia tietystä jakelijasta. Se kuitenkin aiheuttaa lisäkustannuksia. [8.]

Allen listaa kirjassaan useita epäilyttävän liikenteen tunnusmerkkejä [6]. Tässä on esitelty niistä muutamia. Ennen hyökkäystä tapahtuva verkon skannaus voi olla merkkinä yrityksistä tunnistaa verkon laitteiden konfiguraatioita ja Internet-palveluntarjoajia sekä heidän konfiguraatioitaan. Kiinnostavia tietoja hyökkääjälle ovat esimerkiksi isäntäkoneet, käyttöjärjestelmät, verkon topologia ja verkkoon johtavat ulkoista kautta saavutettavissa olevat polut. Yhteydenotot sellaisiin verkon kohteisiin,

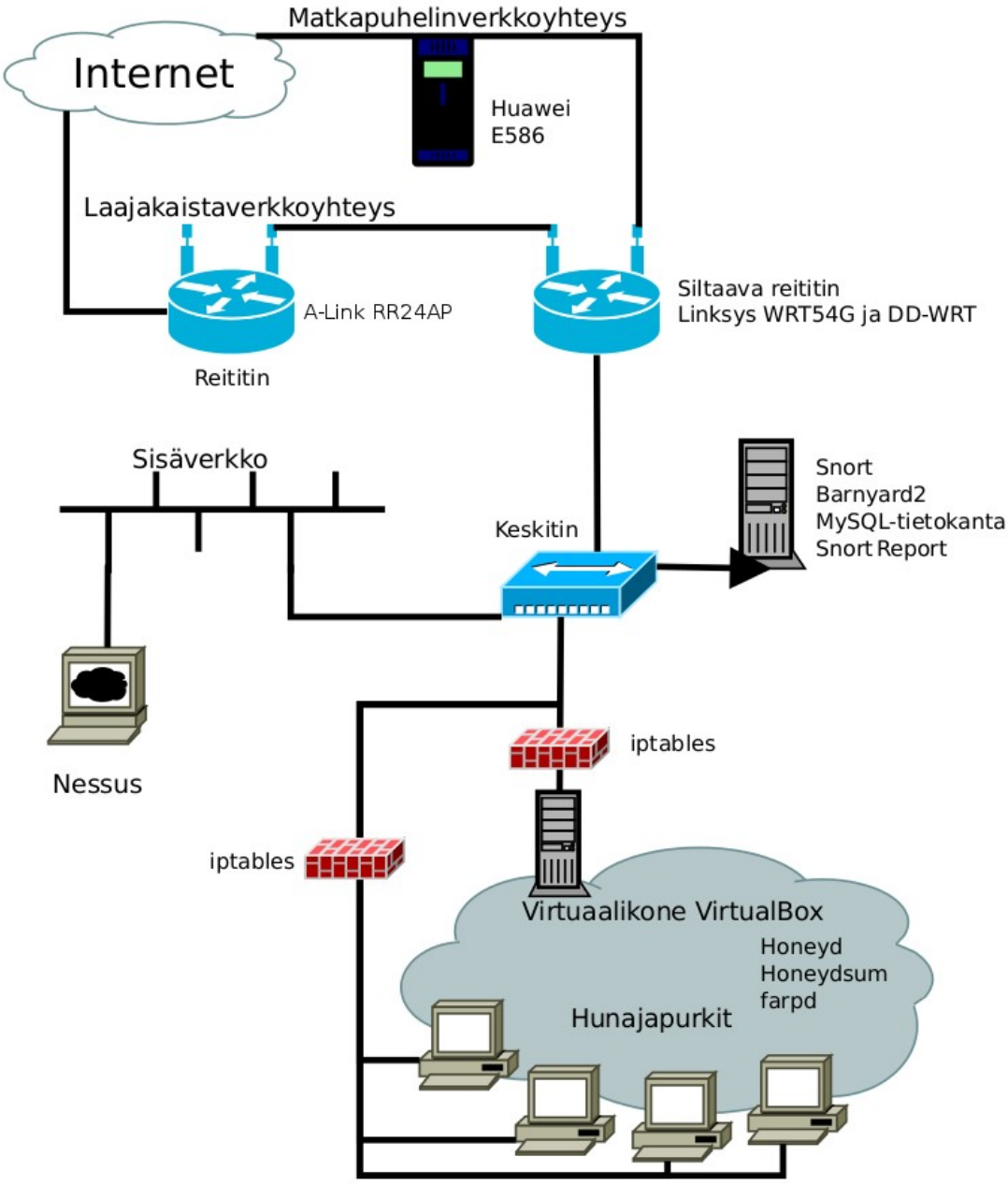
joihin ei normaalisti olla yhteydessä, ovat epäilyttäviä. Protokollaloukkauksia esiintyy usein sen seurauksena, että tunkeutuja käyttää verkkoskanneria ja yrittää ohittaa palomuurin. Jos verkossa esiintyy sellaisia paketteja, joissa lähteen ja vastaanottajan osoitteet ovat verkon ulkopuolelta, se saattaa merkitä sitä, että tunkeutuja on jo verkossa. Epätavalliset porttiyhdistelmät TCP- ja UDP-paketeissa saattavat merkitä sitä, että verkossa ajetaan jotain epätavallista palvelua, kuten takaoviohjelmaa. Yhdestä osoitteesta useisiin eri osoitteisiin suunnatut paketit merkitsevät usein sitä, että tunkeutuja yrittää saada selville palomuuripolitiikan ja palvelut, joita järjestelmä tarjoaa. Epätavallinen ARP-liikenne voi merkitä ARP-väärennöstä. Huomioitavia ovat myös epätavallisen protokollan tai porttinumeron sisältävät paketit, jotka on lähetetty yleisjakeluosoitteisiin. Tällainen liikenne voi merkitä DoS-hyökkäystä. [6.]

4 LAITTEET JA OHJELMAT

Tämä luku esittelee toteutetun tutkimuksen tutkimusympäristöjä sekä siinä käytettyjä laitteistoja ja ohjelmistoja. Tässä esiteltäviä laitteistoa ovat Huawei E586 USB-modeemi ja langaton tukiasema, ja Linksys WRT54G v.5,1-reititin. Esiteltäviä ohjelmistoja ovat Linksys-reitittimeen asennettava DD-WRT-ohjelmisto, hunajapurkkiohjelmisto Honeyd, hunajapurkkikonetta virtualisoiva Oracle VM VirtualBox ja Honeyd-lokien tulkintaohjelma Honeydsum. Esitellään myös tunkeutumisen havaitsemisjärjestelmä Snort ja sen tuottamaa hälytysdataa käsittelevä Barnyard2. Lisäksi esitellään selain-pohjaista Snort-hälytysten tarkasteluohjelmaa Snort Report, verkkohyökkäyksen jäljittelemisessä käytettyä Nessus-tietoturvaskanneria ja Snort-hälytysten tallentamiseen käytettyä MySQL-tietokantaa. Lopuksi esitellään verkon havainnointiin käytetyn järjestelmän kokoonpanoa ja käytettyjen ohjelmistojen käyttöä.

Näillä ohjelmistoilla pyrittiin rakentamaan verkonhavainnointijärjestelmä, joka kykenee havaitsemaan selkeät hyökkäykset ja verkkoon tulevan ylimääräisen liikenteen, sekä tuottamaan liikenteestä sellaista dataa, jota voidaan helposti tarkastella ja josta voidaan pyrkiä vetämään johtopäätöksiä. Ohjelmistojen asentaminen kuvataan yksityiskohtaisesti liitteissä 1 ja 2.

Kuvassa 4-1 on laitteiston yleiskuva. Osassa tutkimustapauksia yhdistettiin havainnointiverkko Internetiin käyttäen 3G-matkapuhelinverkkoliittymää ja osassa käyttäen reititintä. Langaton siltaava reititin mahdollisti keskittimen yhdistämisen langattomaan matkapuhelinverkkotukiasemaan sekä laitteiston sijoittamisen etäälle langattomasta reitittimestä. Tunkeutumisen havaitsemisjärjestelmä Snort ja Honeyd-hunajapurkkikone yhdistettiin keskittimellä toisiinsa. Keskitin yhdistettiin langattomaan siltaavaan reitittimeen.



Kuva 4-1. Yleisverkkokuva kaikista verkon laitteista ja ohjelmista.

4.1 Huawei E586

Huawei E586 on 3G matkapuhelinverkkotukiasema ja langaton reititin, jossa on viiden yhtäaikaa toimivan laitteen tuki. Laitteeseen asetetaan SIM-kortti, jolloin se voi käyttää matkapuhelinverkkoa.

Tukiasema sisältää muun muassa palomuurin, virtuaalipalvelimen ja DMZ-alueen määrittelyn. Näistä palomuuri asetettiin havainnointijaksojen ajaksi pois päältä.

Hunajaverkkotapauksen ja virtuaalipalvelintapauksen havainnointijaksoissa virtuaalipalvelimelle asetettiin reitit hunajapurkkien tarjoamiin palveluihin.

DMZ-alueen käyttö vaati DHCP-palvelimen käyttöönoton reitittimen asetuksista. Matkapuhelinverkkotapauksessa hunajapurkki asetetaan DMZ-alueelle ilman palomuurin suojaa.

4.2 Linksys WRT54G v5,1 ja DD-WRT

Matkapuhelinverkko- , virtuaalipalvelin- ja hunajaverkkotapauksissa Linksys-reititintukiasema toimii langattomana siltaavana reitittimenä. Se yhdistää Huawei-matkapuhelinverkkotukiaseman ja hunajapurkit sekä tunkeutumisen havaitsemisjärjestelmän sisältävän verkon. Laajakaistaverkkotapauksessa se yhdistettiin ADSL-yhteydellä Internetiin yhteydessä olleeseen A-Link RR24AP reitittimeen. Linksys-reititinmallin ohjelmisto ei tukenut siltausta, joten siihen asennettiin DD-WRT v24-sp2 micro-ohjelmisto.

DD-WRT on yksityiskäytössä ilmainen Linux-pohjainen ohjelmisto langattomille reitittimille. Kyseessä on alkuperin Sebastian Gottschallin kehittämä ohjelmisto, jolla on suuri käyttäjäkunta, joten mahdolliset virheet ohjelman toiminnassa löydetään nopeasti. Sen avulla reitittimen ominaisuuksia saadaan laajennettua ja se mahdollistaa laitteen yksityiskohtaisemman hallinnan. On tärkeää tietää reitittimen nimi ja versionumero ennen ohjelmiston asentamista, sillä väärien ohjelmistopakettien asentaminen tekee reitittimestä korjauskelvottoman. Lisää tietoa DD-WRT-ohjelmiston asentamisesta löytyy [9].

4.3 Honeyd

Honeyd on Niels Provosin luoma avoimen lähdekoodin ohjelmisto. Se luo virtuaalisia koneita verkkoon ja niitä yhdistelemällä voidaan muodostaa laajoja hunajaverkkokokonaisuuksia. Honeyd-hunajapurkit voidaan sijoittaa olemassa olevan verkon sellaisiin IP-osoitteisiin, joihin ei ole sijoitettu muita koneita, taikka ne voidaan sijoittaa täysin omaan verkkoonsa. Jokaiselle hunajapurkille asetetaan IP-osoite, määritellään avoimet portit ja niihin palvelut. [1.]

Jotta verkkoliikenne kulkee Honeyd-hunajapurkkiin, on verkko asetettava siten, että virtuaalisille hunajapurkeille osoitettu liikenne kulkee Honeyd isäntäkoneelle. Honeyd vastaa verkkopaketteihin, joiden kohdeosoite kuuluu simuloituihin hunajapurkkeihin. Tämä saavutetaan käyttämällä farpd-ohjelmaa, jolla luodaan hunajapurkkien arp-vastauksia. [1. s.113]

Farpd

Farpd on ohjelma, joka kuuntelee ARP-pyyntöjä ja vastaa asettamattomien IP-osoitteiden puolesta. Käyttämällä farpd-ohjelmaa Honeyd-hunajapurkkiohjelmiston rinnalla on mahdollista täyttää tuotantoverkon tyhjä osoiteavaruus virtuaalihunajapurkeilla.

Farpd saattaa häiritä verkon DHCP-palvelinta saamalla Honeyd-hunajapurkit vastaamaan ICMP-viesteihin, joita DHCP palvelin käyttää selvittämään onko IP-osoite vapaa. Farpd-ohjelman varaamat IP-osoitteet unohtuvat niiden ollessa toimettomina pitkään tai jos osoitteet otetaan käyttöön verkossa. Lisätietoa Ubuntu-Linuxin manuaalissa [16.].

4.4 Honeydsum

Honeydsum on Lucio Henrique Francon ja Carlos Henrique Peixoto Caetano Chavesin kirjoittama ohjelma. Se lukee Honeyd-ohjelman lokitiedostoja ja esittää niistä kerätyt tiedot tekstipohjaisena yhteenvetona. Lokitiedostoista saadaan kerättyä erilaisia tietoja vaihtelemalla ohjelman parametreja. Ne toimivat suodattimina, jolloin lokitiedostoista saadaan muun muassa portteja, IP-osoitteita, liikenteen määriä ja liikenteen ajankohtaan liittyviä tietoja. Ohjelmassa voidaan samanaikaisesti käyttää useita Honeyd-lokitiedostoja, jolloin voidaan yhdistää useampia mittauksia laajemman kokonaiskuvan saamiseksi.

Honeydsum kykenee myös luomaan Honeyd-lokeista graafisen esityksen HTML-sivuna, joka on luettavissa selaimella. Se voi kuvata tapahtumia sekä hunajapurkkikohtaisesti, että useaan hunajapurkkiin kohdistuneen liikenteen yhteenvetona.

4.5 Oracle VM VirtualBox

Virtuaalikonetta käyttäen voidaan suojata isäntäkonetta siltä varalta, että hunajapurkki saadaan murretuksi ja sen hallinta menetetään. Tässä työssä käytettiin VirtualBox-virtuaaliympäristöä, johon asennettiin Ubuntu 12.04 LTS käyttöjärjestelmä Honeyd hunajapurkkien ympäristöksi.

Tässä työssä käytettiin virtuaalikonetta sillatussa tilassa. Siinä isäntäjärjestelmä toimii läpinäkyvänä siltana virtuaalikoneelle. Kaikilla virtuaalihunajapurkeilla on oma IP-osoitteensa, ja ne näkyvät verkossa erillisinä koneina. Virtuaalikoneelle voidaan valita käyttöön DHCP-palvelin tai manuaalinen IP-osoitteen valinta.

Virtuaalikoneen verkkoliitäntä on vuorovaikutuksessa isäntäkoneen verkkoliitännän kanssa ja käyttää sitä lähettämään pakettejaan paikallisverkkoon. Isäntäjärjestelmä

reitittää kaikki virtuaalikoneille tarkoitetut paketit oikeaan kohteeseen. Koko prosessi on läpinäkyvä virtuaalikoneille ja hyökkääjän on verkosta käsin vaikea tunnistaa, onko koneella ajossa virtuaalikone vai ei. [1. s.27]

4.6 Snort

Snort on Sourcefire-yrityksen [30.] kehittämä avoimen lähdekoodin tunkeutumisen havaitsemisjärjestelmä. Se kerää lokitiedostoja verkon tapahtumista sille määriteltyjen sääntöjen perusteella.

Versiosta 2.9.4.0 lähtien Snort ei enää tue suoraan tietokantaan tallentamista vaan se käyttää unified2-ulostuloa. Barnyard2 lukee Snortin unified2-tiedostoa ja toimii sen ja tietokannan välisenä siltana. Barnyard2 lisää tietokantaan Snortin lokista uudet tapahtumat.

Snort voi käyttää itse määriteltyjä sääntöjä tai kuten tässä työssä Sourcefire Vulnerability Research Team-ryhmän määrittelemiä ja ylläpitämiä dynaamisia sääntöjä. Tässä työssä käytettyjen sääntöjen versio on 2.9.4.0 [11.]. Sääntöjen versionumeron tulee olla sama kuin Snort-ohjelman versionumero. Voidaan myös käyttää erilaisia sääntöjä sekaisin ja muokata niitä omiin tarkoituksiin sopiviksi. Dynaamiset säännöt määrittelevät, miten Snort tunnistaa hyökkäykset ja minkälaisesta liikenteestä se tuottaa hälytyksen. Ne perustuvat hyökkäyskuvioiden tunnistukseen sekä protokollien ja epätavallisen liikenteen tarkasteluun.

4.7 Snort Report

Snort Report on Symmetrix Technologies-yrityksen [13.] kehittämä selainpohjainen käyttöliittymä Snort-hälytyksistä luodulle tietokannalle. Sillä voidaan tarkastella Snort-hälytyksiä halutuissa ajanjaksoissa. Se listaa hälytykset tunnisteittain ja tarjoaa mahdollisuuden erikseen tarkastella niihin liittyviä tietoja, kuten lähde- ja kohdeosoitteita, ja sisältöä heksadesimaali- ja tekstimuodossa. Lisäksi Snort Report tarjoaa ehdotuksia mahdollisista lähdemaista, jotka on selvitetty traceroute-työkalulla.

Snort Report ilmoittaa jokaisen hälytyksen kohdalla siihen liittyvän tunnisteen. Jos kyseessä on tunnettu haavoittuvuus tai hyökkäys, se linkittää verkossa ylläpidettyihin haavoittuvuustietokantoihin.

4.8 Barnyard2

Barnyard2 on Ian Firnsin kokoama ilmainen ohjelmisto [14.], joka toimii tulkkina Snort-ohjelmiston tuottamaan unified2-tiedostoon. Se poistaa Snortilta tarpeen käydä läpi tuottamaansa binääridataa ja sen muokkaamisen eri formaatteihin, jolloin olisi

mahdollista, että Snort ei ehtisi huomaamaan kaikkea verkkoliikennettä. Barnyard2 tekee binääridatan käsittelyn Snort-ohjelmiston puolesta vähentäen sille koituvaa rasitusta. [15.]

Barnyard2 pitää kirjanmerkkiä lukemistaan Snort-hälytyksistä waldo-tiedostossa. Mikäli Barnyard2-ohjelmisto sammuu tai jumiutuu, se kykenee jatkamaan oikeasta kohdasta kirjanmerin ansiosta. Näin se ei hukkaa alhaalla-oloaikana tulleita hälytyksiä. Tiedot se siirtää tietokantaan, jonne on luotu Snort-hälytyksiä vastaavat kentät. [15.]

4.9 Nessus 5.1

Nessus on verkossa olevien palvelimien ja palvelujen turvallisuuden testaamiseen kehitetty ohjelmisto. Se on Tenable Network Security-yrityksen tuottama ja siitä on olemassa ilmainen ja maksullinen versio. Maksulliseen on saatavilla enemmän toimintoja ja lisäosia [12]. Nessus käyttää osana toimintaansa myös nmap-verkkoskanneria, jolla voidaan tarkastaa verkossa olevien koneiden avoimet portit ja palvelut. Sitten se kokeilee erilaisia haavoittuvuuksia avoimille porteille. Nessus-järjestelmä sisältää tietoturvapalvelimen tarkistusten suorittamista varten. Se hyödyntää testausten tekemisessä tietokantaa, joka sisältää tietoja tunnetuista turva-aukoista. [7.]

Haavoittuvuusskannaus tuottaa kattavia ja monipuolisia raportteja. Tarkistusskannaukset rasittavat kohteena olevia järjestelmiä ja voivat aiheuttaa niiden toimintojen häiriintymisen. Skannauksen asetuksia muokkaamalla voidaan sen rasittavuutta vähentää taikka lisätä tarkoituksiin sopivaksi. [7.]

4.10 MySQL-tietokanta

MySQL-tietokanta on Oraclen omistama relaatiotietokantaohjelmisto. Se on saatavissa ilmaisesti vapaalla GNU GPL-lisenssillä taikka vaihtoehtoisesti kaupallisella lisenssillä. Tutkimuksesa käytetty MySQL versio oli 5.5.29. [31.]

MySQL-tietokanta asennettiin Snort-ohjelmiston yhteyteen. Se voidaan sijoittaa myös muualle verkkoon, ja Snort voidaan asettaa lähettämään hälytystietoja tietokantapalvelimelle [3. s.158]. Uusissa Snort-ohjelmiston versioissa se tuottaa unified2 tyyppistä ulostuloa, joten tarvitaan Barnyard2 taikka vastaava ohjelma käsittelemään tietoa. Barnyard2 syöttää Snort-hälytykset MySQL-tietokantaan.

4.11 Laitteet ja ohjelmat verkossa

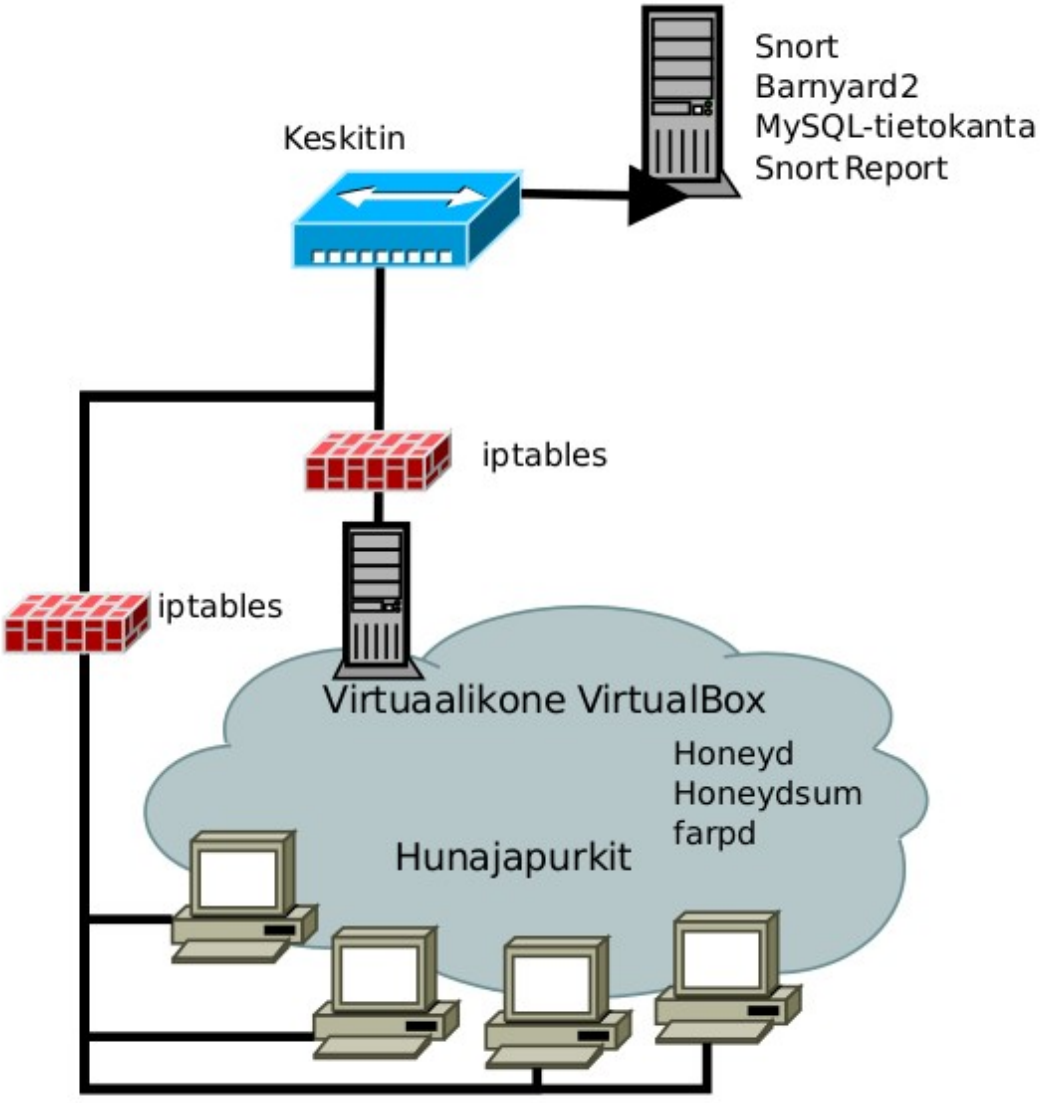
Havainnointijärjestelmä koostuu tunkeutumisen havaitsemisjärjestelmästä Snortista ja Honeyd-hunajapurkkiohjelmistosta. Nämä kaksi ohjelmistoa sijaitsevat verkon kahdessa eri koneessa. Ne on fyysisesti yhdistetty ethernetverkon keskittimeen.

Toiselle tietokoneelle asennettiin VirtualBox-virtuaalikone virtualisoimaan Ubuntu-Linux konetta. Kuvassa 4-2 on esitelty havainnointijärjestelmän yleinen kokoonpano. Honeyd-hunajapurkki sijaitsee VirtualBox-ohjelmiston virtuaalikoneella ja se puolestaan sijaitsee isäntäkoneella. Virtuaalikone toimii turvallisena hiekkalaatikkona hunajapurkkeille. Honeyd-ohjelmiston mukana tuli myös Honeydsum-ohjelma, jota käytetään lokitiedostojen tulkintaan. Farpd-ohjelma on asennettu virtuaalikoneelle Honeyd-ohjelmiston yhteyteen. Sen tehtävänä on luoda hunajapurkeille ARP-osoitteet ja ohjata niille osoitettu verkkoliikenne perille. Fyysisen isäntäkoneen verkkoliitännät asetettiin katkaistu-tilaan. Tällä vältetään turha liikenne sen ja hunajapurkin välillä. VirtualBox-ohjelmisto on asetettu siltaamaan liikenne isäntäkoneen verkkoliitäntää käyttäen sen isännöimälle virtuaalikoneelle. Virtuaalikoneen kannalta tämä on sama kuin suora fyysinen yhteys verkkoon [1. s.27]. Isäntäkone on yhdistetty ethernet-kaapelilla keskittimeen.

Toisesta tietokoneesta tehtiin tunkeutumisen havaitsemisjärjestelmä asentamalla siihen Snort ja sen yhteyteen Barnyard2, MySQL-tietokanta ja Snort Report. Näillä ohjelmilla saadaan Snort-hälytykset talletettua tietokantaan ja niitä kyetään tarkastelemaan webselaimella. Snort yhdistettiin hunajapurkkilaitteiston kanssa samaan keskittimeen. Se käyttää verkkoliitäntää ilman IP-osoitetta, jolloin se ei osallistu tietoliikenteeseen millään tavoin. Se kuitenkin vastaanottaa kaiken verkkoon saapuvan tietoliikenteen. Näin Snort-ohjelmisto kuuntelee verkkoa passiivisesti.

Käyttämällä ethernet-liitäntää voidaan keskitin yhdistää tässä työssä toteutettuihin verkkorakenteisiin. Sisäverkkotapauksessa yhdistettiin keskitin suoraan olemassa olevaan verkkoon. Muissa tapauksissa keskitin yhdistettiin siltaavaan reitittimeen, joka toimi langattomana yhteytenä toisen reitittimen välillä.

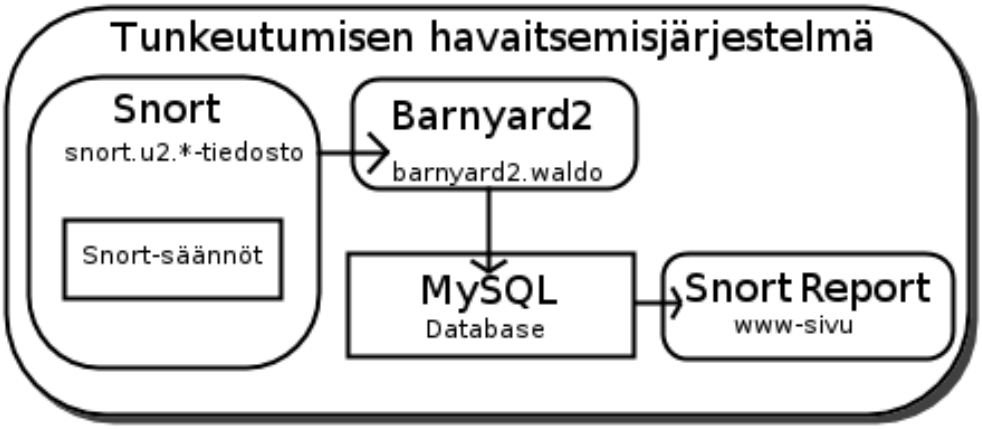
Linux käyttöjärjestelmää virtuaalisoivan koneen ja hunajapurkkia ajavan virtuaalikoneen suojaamiseksi käytettiin iptables-palomuuria. Sillä rajoitettiin tietoliikennettä siten, että ainoastaan hunajapurkkeihin kulkeva ja niiltä lähtevä liikenne on sallittua.



Kuva 4-2. Havainnoinnissa käytetyt työkalut.

4.11.1 Tunkeutumisen havaitsemisjärjestelmä

Kuvassa 4-3 on esitetty Snort ja sen kanssa toimivat ohjelmat suhteessa toisiinsa. Snort-koneelle on asennettu tunkeutumisen havaitsemisjärjestelmä Snort, Barnyard2-ohjelmisto, MySQL-tietokanta ja Snort Report-ohjelmisto. Barnyard2 lukee Snort-ohjelmiston hälytyksistä tuottamaa unified2-ulostulo-tiedostoa ja tallentaa siitä hälytys-tiedot MySQL-tietokantaan. Snort Report lukee hälytys-tietokantaa ja näyttää tiedot websivuna.



Kuva 4-3. Tunkeutumisen havaitsemisjärjestelmä ja siihen liittyvät ohjelmat.

Tunkeutumisen havaitsemisjärjestelmä Snortin ja Barnyard2-ohjelman asennuksesta ja asetuksista tarkemmin liitteessä 1. Kuvassa 4-4 on Snort-ohjelman käynnistyskomento ja kuvassa 4-5 on Barnyard2-ohjelman käynnistyskomento. Lisää tietoa komennoista ja niiden optioista löytyy ohjelmien ohjeista [15;17;18].

```
sudo /usr/local/snort/bin/snort  -u  snort -g snort -c /usr/local/snort/etc/snort.conf -i eth0

  -u Asettaa Snort-ohjelman toimimaan seuraavan käyttäjän alaisena
  -g Vaihda Snort-ohjelma toimimaan seuraavan ryhmän alaisena
  -c Käytä sääntöjä tästä asetus tiedostosta
  -i Tarkkaile tätä verkkoliitäntää
```

Kuva 4-4. Snort-ohjelman käynnistyskomento.

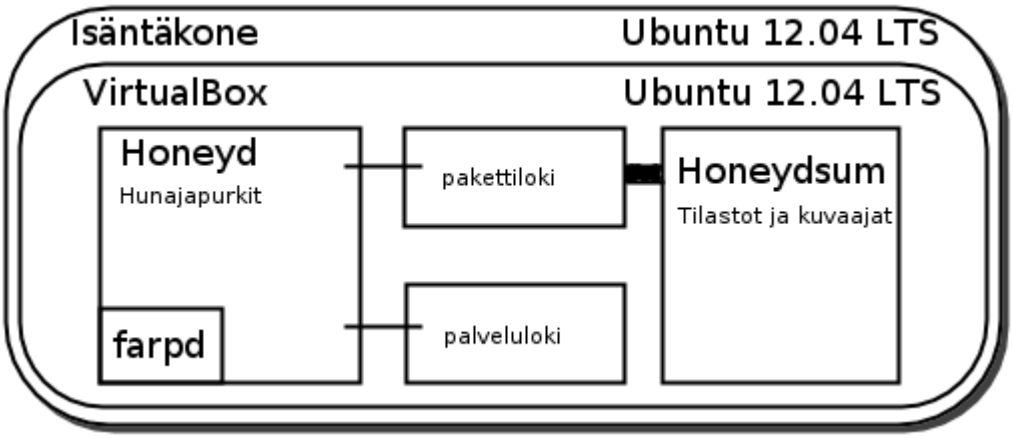
```
sudo /usr/local/bin/barnyard2  -c /usr/local/snort/etc/gen-msg.map  -S /usr/local/snort/etc/sid-msg.map
-d /var/log/snort/ -f snort.u2  -w /var/log/snort/barnyard2.waldo
  -c Asetustiedosto
  -S Lue sid-msg kartta tästä tiedostosta
  -d kerää tiedostoja täältä
  -f käytä tätä tiedostonimen alkuna
  -w Salli kirjanmerkintä käyttäen tätä tiedostoa
```

Kuva 4-5. Barnyard2-ohjelman käynnistyskomento.

4.11.2 Hunajapurkki

Kuvassa 4-6 on esitetty hunajapurkkikoneen ohjelmat suhteessa toisiinsa. Isäntäkoneelle on asennettu VirtualBox-ohjelmisto, joka jäljittelee virtuaalista Ubuntu-Linux

ympäristöä. Tähän virtuaaliympäristöön on asennettu Honeyd-hunajapurkkiohjelmisto. Lisäksi Honeyd-ohjelmiston yhteyteen on asennettu farpd- ja Honeydsum-ohjelmat.



Kuva 4-6. Hunajapurkkiasetelman laitteet ja ohjelmat.

Honeyd-hunajapurkkiohjelmisto asetettiin kuuntelemaan verkkoliitäntää ja käytettiin farpd-ohjelmistoa luomaan hunajapurkille arp-osoitteet. Honeyd-hunajapurkit määriteltiin asetustiedostoissa. Asetustiedoston sisällöstä tarkemmin liitteessä 3. Kuvassa 4-7 on Honeyd-ohjelmiston käynnistyskomento

```
sudo honeyd -d -i eth0 -f /usr/local/Honeyd/Honeyd_conf/laajakaista.conf
-l /tmp/pakettiloki.log -s /tmp/palveluloki.log
  -d Älä aja daemonina. Salli tekstimuotoinen viestien tarkastelu
  -i Kuuntele tätä verkkoliitäntää
  -f Lue asetustiedosto täältä
  -l Pidä lokia paketeista ja yhteyksistä tähän tiedostoon
  -s Pidä lokia palveluista tähän tiedostoon
```

Kuva 4-7. Honeyd-ohjelman käynnistyskomento.

Tässä työssä Honeydsum-ohjelmaa käytetään tuottamaan helpommin tulkittavaa tietoa lokitiedostoista. Honeydsum tuottaa Honeyd-ohjelmiston pakettilokitiedostoista yhteenvedon. Se suodattaa lokitiedostot halutusti ja antaa hunajapurkki kohtaista tietoa liikenteestä. Sille voidaan syöttää useita lokitiedostoja samanaikaisesti. Kuvassa 4-8 on Honeydsum-ohjelman käynnistyskomento:

```
sudo ./honeydsum.pl -c honeydsum.conf [-hVw] log-tiedosto1 log-tiedosto2 ...

  -c Honeydsum asetustiedosto
  -h Näytä optiotiedot ja lopeta
  -V Näytä versionumero ja lopeta
  -w Näytä ulostulo HTML-sivuna
```

Kuva 4-8. Honeydsum-ohjelman käynnistyskomento.

Virtuaalikonetta ajava isäntäkone ja virtuaalikone suojattiin käyttämällä iptables-palomuuria. Isäntäkoneelle säännöt asetettiin siten, että kaikki sille suuntautuva liikenne pudotettiin. Kuvassa 4-9 on sääntöjen luomiseen käytetyt komennot.

```
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
```

Kuva 4-9. Isäntäkoneen palomuurikomennot.

Virtuaalikoneelle luotiin säännöt, jotka sallivat ainoastaan hunajapurkkien osoitteisiin saapuvan liikenteen. Ulospäin suuntautunut liikenne sallittiin, jotta koneelle voitaisiin haluttaessa luoda hälytyksistä ilmoittava sähköpostitoiminto. Kuvassa 4-10 virtuaalikoneelle luodut iptables-palomuurin sääntöjen luomiseen käytetyt komennot.

```
sudo iptables -A INPUT -d 192.168.1.111 -j ACCEPT
sudo iptables -A INPUT -d 192.168.1.112 -j ACCEPT
sudo iptables -A INPUT -d 192.168.1.113 -j ACCEPT
sudo iptables -A INPUT -m state -state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
```

Kuva 4-10. Virtuaalikoneen palomuurikomennot.

5 TUTKIMUSYMPÄRISTÖ

Tässä luvussa tarkastellaan tutkimuksen toteutusta ja testausta sekä tutustutaan käytettyihin verkkorakenteisiin. Toteutettiin viisi verkkorakennetta mukaillen luvussa 2 esitettyjä hunajapurkkien sijoituspaikkoja.

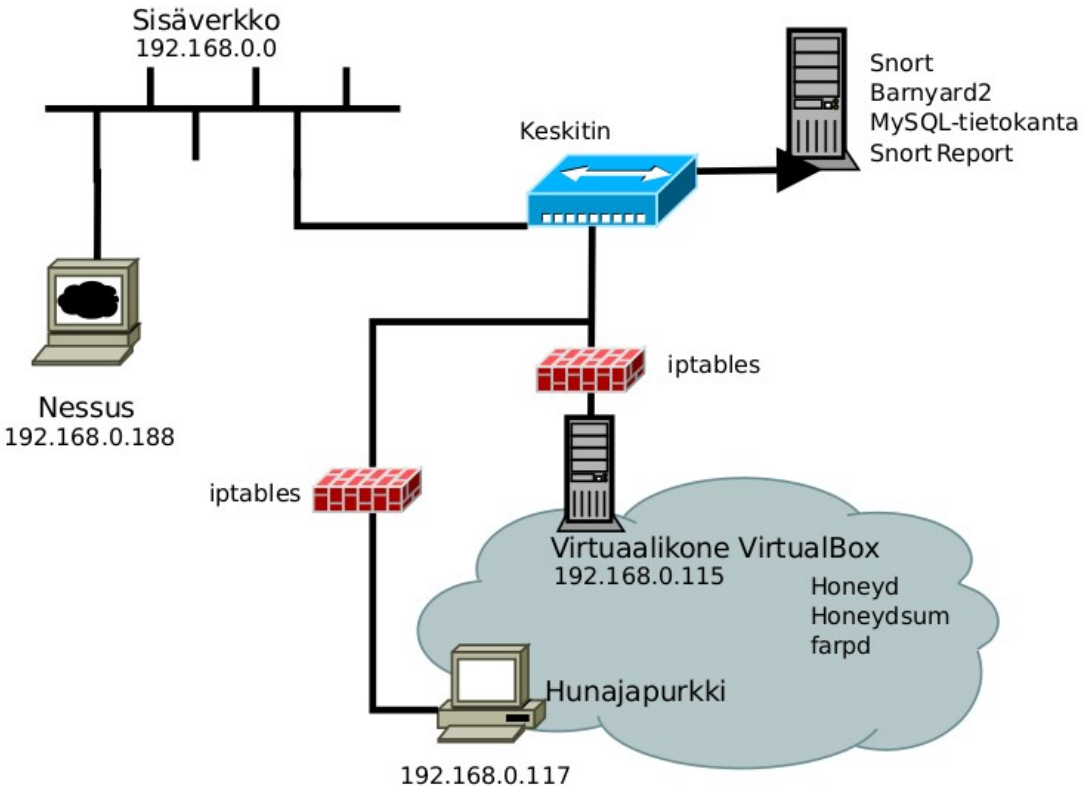
Ensimmäinen tapaus oli sisäverkossa tapahtuva hyökkäys. Sitä jäljiteltiin suorittamalla Nessus-haavoittuvuusskannerilla koko sisäverkon kattava turvallisuusskannaus. Hunajapurkki ja tunkeutumisen havaitsemisjärjestelmä-yhdistelmä asetettiin osaksi sisäverkkoa skannauksen ajaksi. Toinen tapaus oli laajakaistaverkko, jossa havainnointijärjestelmä sijoitettiin ADSL-yhteydellisen reitittimen DMZ-alueelle. Reitittimen palomuuri jätettiin päälle, jotta voitiin jäljitellä normaalia palomuurilla suojattua aluetta. Kolmannessa tapauksessa havainnointijärjestelmä sijoitettiin matkapuhelinverkkoon yhdistetyn reitittimen DMZ-alueelle. Tässä tapauksessa palomuuri kytkettiin pois päältä. Neljännessä ja viidennessä tapauksessa havainnointijärjestelmä sijoitettiin sisäverkkoon, jonne reitittimen virtuaalipalvelin ohjasi liikennettä matkapuhelinverkosta. Viidennessä tapauksessa sisäverkkoon toteutettiin kolmen koneen hunajaverkko.

Lopuksi esitellään tutkimuksessa käytettyjen hunajapurkkien asetetukset. Käydään läpi avoimet portit ja jäljitellyt palvelut.

5.1 Sisäverkko

Tässä tapauksessa haluttiin tarkkailla organisaation sisäistä verkkoa sisäisen uhkatekijän tehdessä verkkoon hyökkäystä. Hyökkäystä simuloitiin tekemällä koko sisäverkon skannaus Nessus-tietoturvaskannerilla. Havainnointijakson pituus oli puolitoista tuntia.

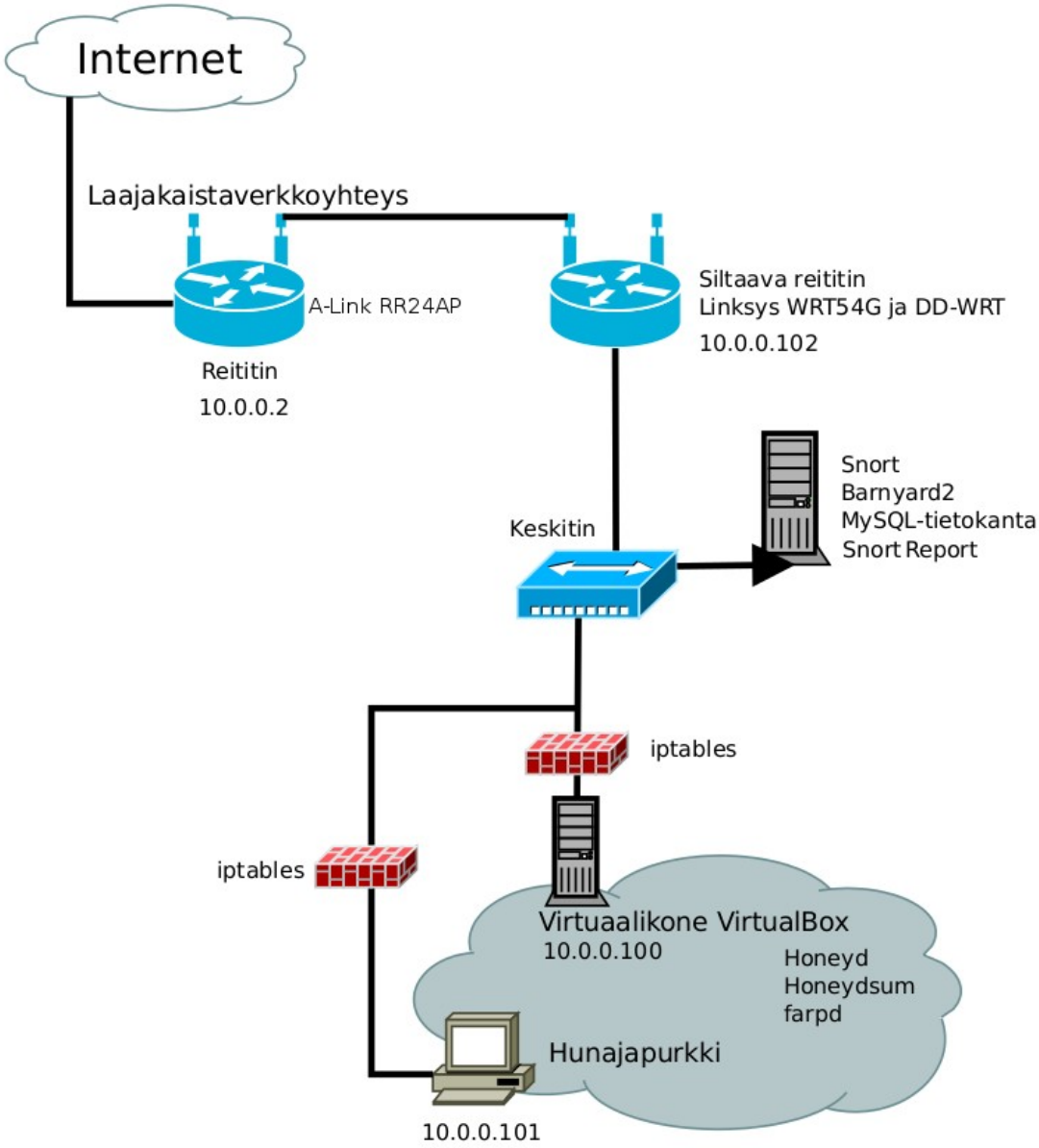
Tunkeutumisen havaitsemisjärjestelmä Snort ja Honeyd-hunajapurkki liitettiin osaksi paikallisen organisaation sisäverkkoa 192.168.0.0/24. Hunajapurkille annettiin IP-osoite 192.168.0.117 ja hunajapurkkia isännöivälle virtuaaliselle VirtualBox-koneelle 192.168.0.115. Kuvassa 5-1 on esitelty sisäverkon rakenne kattaen havainnointijärjestelmän sekä hyökkäyksen suorittavan Nessus-koneen. Nessus-tietoturvaskanneri asennettiin verkon IP-osoitteessa 192.168.0.188 sijaitsevaan tietokoneeseen. Käytettiin skannerin valmiiksi määriteltyä sisäverkkojen oletustestausskannausta ja kohdistettiin se koko 192.168.0.0/24 verkkoon.



Kuva 5-1. Sisäverkkotapauksen verkkorakenne.

5.2 Laajakaistaverkko

Laajakaistaverkkotapauksessa haluttiin havainnoida verkon ulkopuolelta tapahtuvaa hyökkäystä palomuurilla suojattuun DMZ-alueen laitteeseen. A-Link-reittimen asetuksista sisääntulevan liikenteen oletus toiminto astetettiin esto-tilaan. Havainnointijakson pituus oli kahdeksan vuorokautta. Havainnointijärjestelmä sijoitettiin ADSL-yhteydellä Internetiin yhdistetyn reitittimen DMZ-alueelle. Kuvassa 5-2 nähdään laitteiden IP-osoitteistus ja verkonrakenne. Havainnointijärjestelmä on yhdistetty langattoman siltaavan reitittimen kautta reitittimelle. Hunajapurkin IP-osoitteeksi asetettiin verkon osoitteistuksen mukaisesti 10.0.0.101 ja virtuaalikoneen IP-osoitteeksi asetettiin 10.0.0.100.



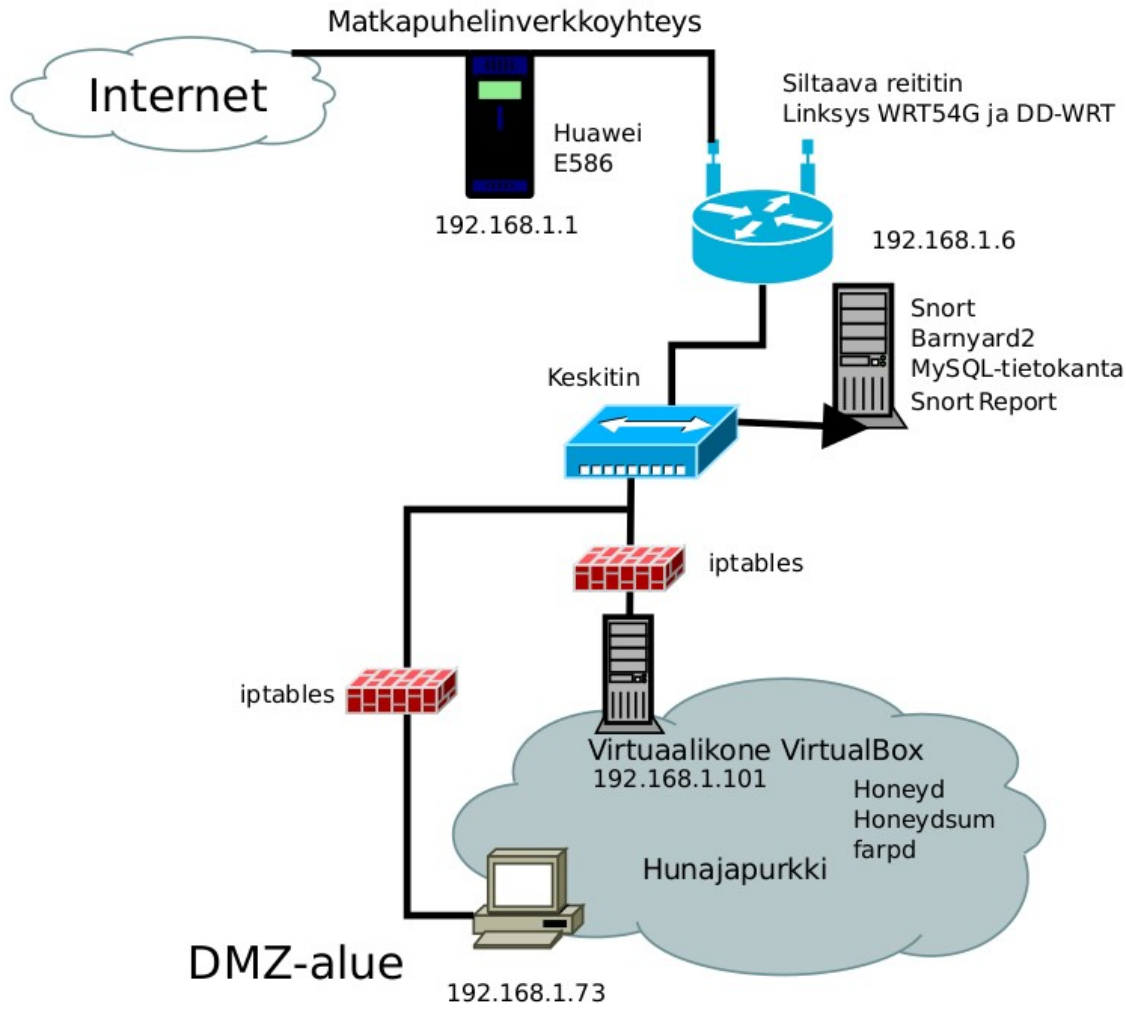
Kuva 5-2. Laajakaistaverkkotapauksen verkkorakenne.

5.3 Matkapuhelinverkko

Tässä tapauksessa tahdottiin havainnoida verkon ulkopuolelta matkapuhelinverkosta tapahtuvaa vihamielistä liikennettä. Havainnointijakson pituus oli yhdeksän vuorokautta. Haluttiin nähdä onko liikenteellä eroa laajakaistaverkkotapaukseen.

Hunajapurkki sijoitettiin reitittimen DMZ-alueelle ilman palomuuria, jolloin kaikki matkapuhelinverkon kautta tuleva liikenne ohjautui sille. Haluttiin havainnoida suoraan matkapuhelinverkkoon yhdistyneeseen laitteeseen kohdistunutta liikennettä.

Kuvassa 5-3 nähdään verkonrakenne ja IP-osoitteistus. Havainnointijärjestelmä on yhdistetty langattoman sillan kautta reitittimeen ja sen kautta matkapuhelinverkkoon.



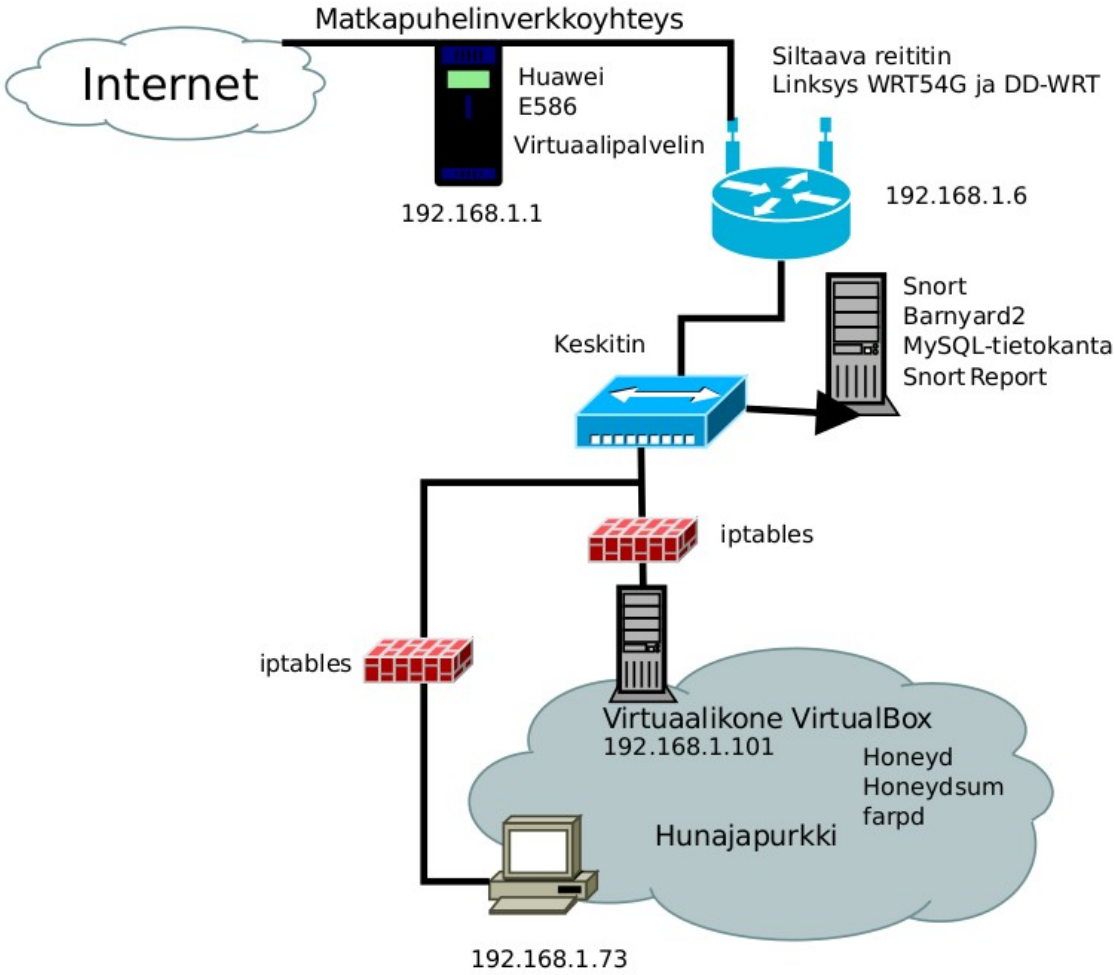
Kuva 5-3. Matkapuhelinverkkotapauksen verkkorakenne.

5.4 Virtuaalipalvelin

Tässä havaintojaksossa asetettiin reitittimen virtuaalipalvelin ohjaamaan hunajapurkkiin ainoastaan sille määritellyn liikenteen. Näin voitiin ohjata liikenne suoraan hunajapurkkien portteihin ja palveluihin. Tämä havainnollistaa tilannetta, jossa verkossa oleva laite on palomuurin suojissa, mutta sille on viihde- tai työtarkoitukseen avattu reittejä tiettyihin palveluihin. Havainnointijakson pituus oli kuusi vuorokautta.

Kuvassa 5-4 esitellään tapauksessa käytetyn verkon rakenne. Se on lähes sama kuin matkapuhelinverkkotapauksessa. Hunajapurkki on tässä sijoitettu DMZ-alueen sijaan

sisäverkkoon, jonne reitittimen virtuaalipalvelimelta on reitti tiettyihin portteihin ja palveluihin.



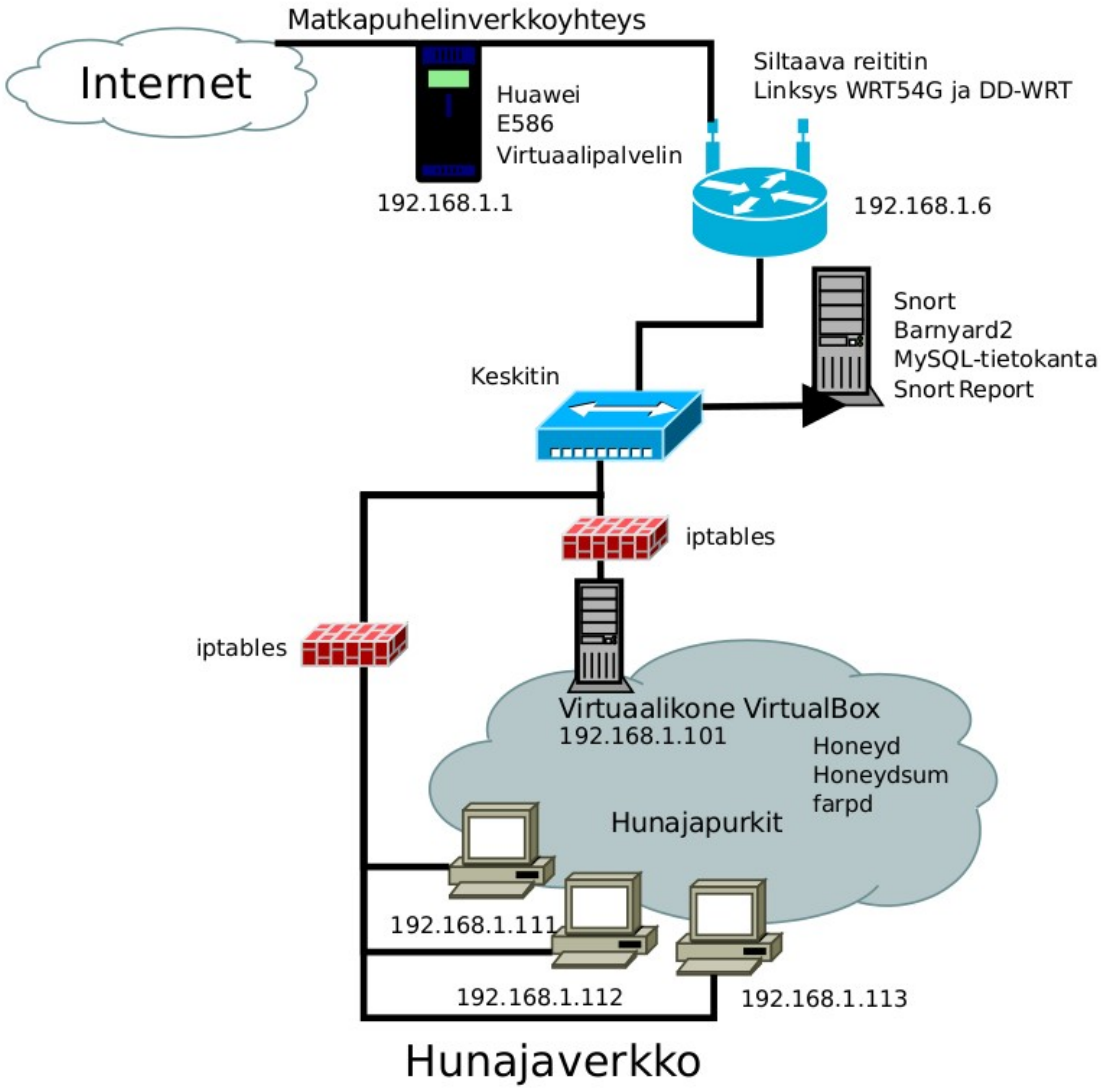
Kuva 5-4. Virtuaalipalvelintapauksen verkkorakenne.

5.5 Hunajaverkko

Virtuaalipalvelintapauksen lisäksi tehtiin samalla verkkorakenteella neljän hunajapurkin hunajaverkko. Tarkoituksena oli tarkastella usean erilaisen hunajapurkin etuja ja haittoja yksittäiseen verrattuna. Tahdottiin myös testata Honeydsum-ohjelman kykyä esittää tietoja usean hunajapurkin verkon liikenteestä. Havainnointijakson pituus oli yksitoista vuorokautta.

Liikenne hunajapurkkeihin ohjattiin reitittimen virtuaalipalvelimelta. Tämä havainnollistaa tilannetta, jossa reitittimeen on yhdistettynä pieni lähiverkko. Reititin toimi lähiverkon yhdyskäytävänä Internettiin ja sen virtuaalipalvelimelta oli avattu

reittejä lähiverkon palveluihin. Kuvassa 5-5 on kuvattu tapauksen verkkorakenne ja siinä käytetyt laitteet IP-osoitteineen.



Kuva 5-5. Hunajaverkkotapauksen verkkorakenne.

5.6 Hunajapurkit

Honeyd-hunajapurkit jäljittelevät käyttöjärjestelmiä vastaamalla yhteydenottoyrityksiin kyseessä olevalle käyttöjärjestelmälle sopivilla tavoilla. Niille asetetaan persoonallisuuksia, jotka vastaavat Nmap- ja Xprobe-verkkoskannereiden tunnistamia sormenjälkiä.

Työn aikana käytettiin kahta eri hunajapurkkiasetelmaa. Ensimmäisessä on yksi Windows-palvelinta jäljittelevä hunajapurkki. Sitä käytettiin kaikissa muissa

tapauksissa paitsi Hunajaverkkotapauksessa. Toisessa on neljän laitteen hunajaverkko ja tätä asetelmaa käytettiin ainoastaan hunajaverkkotapauksessa. Liitteessä 3 löytyy hunajapurkkien asetustiedostot.

Hunajapurkkiasetelma 1

Tätä hunajapurkkiasetelmaa käytettiin lähes kaikissa tapauksissa. Sisäverkko- , laajakaista- , matkapuhelinverkko- ja virtuaalipalvelintapauksissa vaihdetaan ainoastaan hunajapurkille asetettua IP-osoitetta vastaamaan kulloinkin käytössä olevan verkkorakenteen osoitteistusta.

Sen persoonallisuudeksi valittiin Microsoft Windows 2000 Server-palvelin ja sille määriteltiin avoimiksi portit 23, 135, 137, 138, 139 ja 445. Portteihin 21, 25, 110 ja 143 asetettiin niistä todennäköisesti oikeasta koneesta löytyviä palveluita. Porttiin 21 jäljiteltiin FTP-palvelua, porttiin 25 jäljiteltiin SMTP-palvelua, porttiin 110 jäljiteltiin POP3-palvelua ja porttiin 143 jäljiteltiin IMAP-palvelua.

Hunajapurkkiasetelma 2

Tätä hunajapurkkiasetelmaa käytettiin ainoastaan hunajaverkkotapauksessa. Siinä haluttiin tutkia usean hunajapurkin verkon toimintaa verrattuna muissa käytettyyn yhden hunajapurkin verkkoon. Haluttiin myös testata Honeydsum-ohjelman kykyä tuottaa tietoa useasta hunajapurkista.

Hunajapurkki mukailee Honeyd-ohjelmalle saatavissa olevaa valmista asetuspohjaa [29.]. Hunajaverkkoon luotiin Windows 2000 palvelin, Windows Vista-kone, Cisco-reititin ja Ubuntu-Linux-tietokone. Microsoft Windows 2000 Server-palvelinhunajapurkin IP-osoiteeksi asetettiin 192.168.1.111. Sille määriteltiin avoimiksi portit 135, 137 ja 139. Lisäksi porttiin 80 asetettiin emuloitavaksi ISS-web-palvelin. IP-osoitteessa 192.168.1.113 on Microsoft Windows Vista-hunajapurkki. Sen asetukset ovat samat kuin Microsoft Windows 2000-palvelimen. Sille on kuitenkin asetettu Vista-koneen persoonallisuus. Cisco-reititintä jäljittelevän hunajapurkin IP-osoitteeksi asetettiin 192.168.1.112 ja sen portti 23 asetettiin jäljittelemään reitittimen telnet-palvelua. Ubuntu-Linux-hunajapurkin IP-osoitteeksi asetettiin 192.168.1.114. Sen portti 445 asetettiin avoimeksi ja porteihin 21, 25 ja 110 asetettiin oikeita palveluja jäljitteleviä palveluita. Portiin 21 sijoitettiin SSH- , porttiin 25 SMTP- ja porttiin 110 POP3-palveluita jäljittelevät ohjelmat.

6 TULOKSET

Tässä luvussa esitellään ja analysoidaan tutkimuksessa saadut tulokset. Pohditaan erityisesti sitä, kuinka hyvin tutkimuksessa käytetty tunkeutumisen havainnointijärjestelmä ja hunajapurkit toimivat yhteistyössä keskenään sekä sitä, kuinka hyvin käytetyillä työkaluilla kyetään tuottamaan sellaista tietoa, jota voidaan tehokkaasti hyödyntää verkon erilaisten tietoturvariskien kartoittamiseen.

Kaikissa tuloksissa jätettiin mainitsematta ulkopuolisten tekijöiden osoitteet, jotta heidän yksityisyytensä säilyisi. Nämä tekijät eivät välttämättä ole mahdollisten hyökkäysten suorittajia, vaan he voivat olla vain vaarantuneen koneen omistajia. Tarvittaessa niiden osoitteiden tilalla on käytetty kirjaimia.

Tietoa tietoliikenteestä ja hyökkäyksistä kerättiin Honeyd-hunajapurkkien ja tunkeutumisen havaitsemisjärjestelmä Snortin tuottamista loki- ja ulostulotiedostoista. Tulkinnan apuna käytettiin Snort Report- ja Honeydsum-ohjelmia.

Tässä työssä hunajapurkit oli asetettu sellaisille verkon IP-osoitteille, jotka eivät olleet muussa käytössä. Lisäksi hunajapurkeilla ei ollut käyttäjiä eikä niillä ollut mitään tuotanto-ohjelmistoja asennettuina. Siksi voidaan pitää kaikkea hunajapurkeille suuntautunutta tietoliikennettä epäilyttävänä.

Tarkastellaan tuloksia luvussa 5 esiteltyihin tapauksiin jaettuina. Sisäverkkotapauksessa tarkoituksena oli jäljitellä tilannetta, jossa verkkoon on päässyt käsiksi vihamielinen toimija. Laajakaistaverkkotapauksessa havainnoitiin tilannetta, jossa hyökkäys tapahtuu verkon ulkopuolelta. Matkapuhelinverkkotapauksessa havainnoitiin oman verkon ulkopuolelta matkapuhelinverkosta tapahtuvaa vihamielistä liikennettä. Virtuaalipalvelintapauksessa haluttiin tarkastella DMZ-alueella palomuurin suojissa olevalle laitteelle tulevaa liikennettä. Hunajaverkkotapauksessa tahdottiin havainnoida usean erilaisen hunajapurkin etuja ja haittoja yksittäiseen verrattuna.

Tulosten tarkastelun jälkeen tarkastellaan havaintojaksojen yhteenvetoja ja pohditaan tulosten merkitystä. Pyritään saamaan kuva siitä, miten hyvin havainnointi on onnistunut.

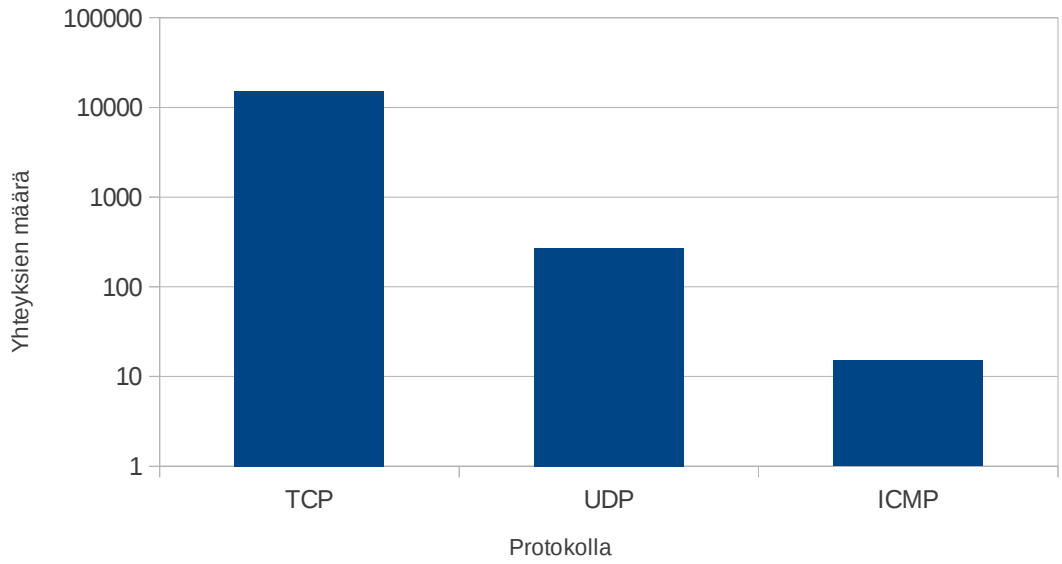
6.1 Sisäverkko

Sisäverkkotapauksessa jäljiteltiin tietoturvahyökkäystä Nessus-tietoturvaskannerilla tehdyllä haavoittuvuusskannauksella. Havainnointiin verkkoa puolitoista tuntia, jolloin Nessus oli ehtinyt suorittaa skannauksensa.

Snort Report-ohjelmalla voidaan nähdä, että samaan aikaan hunajapurkin tallentaman tietoliikennepiikin kanssa tunkeutumisen havaitsemisjärjestelmä Snort on havainnut verkkoon kohdistuneita hyökkäyksiä. Suoraan hunajapurkkiin kohdistunut haavoittuvuusskannaus tuotti suuren määrän lokitietoa. Skannauksen aikana Nessus-skanneri etsi järjestelmän avoimia portteja ja testasi verkon koneiden tunnettuja haavoittuvuuksia. Honeydsum-ohjelma ei kyennyt tuottamaan graafista esitystä näin laajasta joukosta portteja. Sen sijaan sillä tuotettiin tekstimuotoinen yhteenveto, josta taulukkolaskentaohjelman avulla koostettiin kuvaajat. Näistä kuvaajista ja Honeydsum-yhteenvedosta voidaan nähdä hyökkäyksen ajankohta, mistä osoitteesta hyökkäys on suoritettu, käytettyjen protokollien määrä ja mihin portteihin hyökkäyksessä on keskitytty.

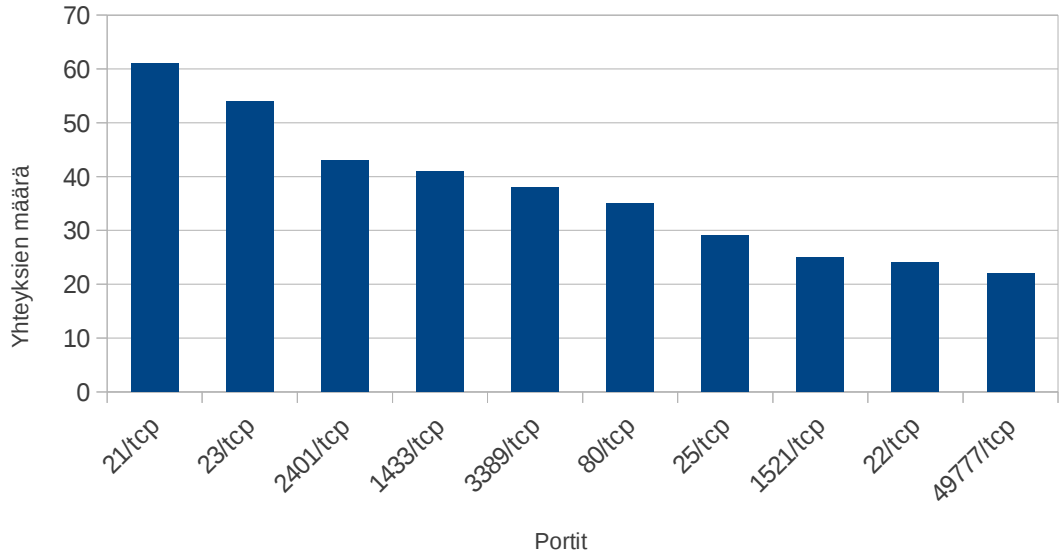
Skannauksen aiheuttaman liikenteen lisäksi verkon muut koneet lähettivät lukuisia yleis- ja ryhmälähetysviestejä, jotka myös kasvattivat hunajapurkin lokitiedostoa. Niitä ei kuitenkaan huomioida yhteenvetoa luotaessa, koska niitä ei ole erityisesti kohdistettu hunajapurkille. Lokitiedostojen kasvu ylimääräisestä liikenteestä on yksi hunajapurkin yhteiseen osoiteavaruuteen sijoittamisen huonoista puolista.

Kuvassa 6-1 on esitetty hunajapurkille suuntautunut liikenne jaettuna käytettyihin protokolliin. Tässä tapauksessa verkossa oli ainoastaan yksi hyökkäävä kone IP-osoitteessa 192.168.0.188. Honeydsum-yhteenvedosta voidaan nähdä haavoittuvuusskannauksen koettaneen 4677:ää erillistä porttia. Kaiken kaikkiaan yhteysyrityksiä hunajapurkkiin oli 15485 kappaletta. Näistä 15199 yhteysyritystä käytti TCP-protokollaa, 271 käytti UDP-protokollaa ja 15 ICMP-protokollaa. Yhteenvedosta nähdään, että ICMP-protokolla paketit olivat porttinumeroihin 8, 13, 17 ja 37. ICMP-viesteissä numero ei tarkoita porttinumeroa vaan se on ICMP-koodi. Numero 8 tarkoittaa Echo-viestiä, numero 13 aikaleimaa, numero 17 osoitepeitteen pyyntö-viestiä ja numero 37 nimipalvelimen pyyntö-viestiä.



Kuva 6-1. Sisäverkossa hunajapurkille saapuneiden pakettien jakautuminen.

Kuvassa 6-2 esitellään portteihin tulleet yhteydet ja yhteys määrät pylväsdiagrammina. Tästä kuvasta voidaan nähdä portteihin kohdistunut liikenne suhteessa toisiinsa.



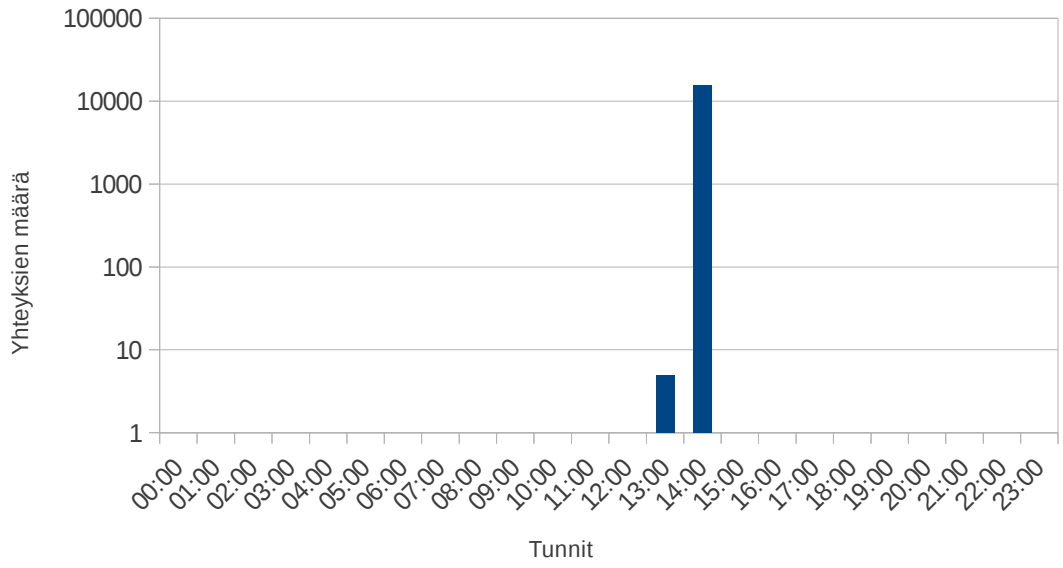
Kuva 6-2. Kymmenen käytetyintä porttia ja niihin tulleiden yhteyksien määrä.

Taulukossa 6-1 on listattu kymmenen haavoittuvuusskannauksessa eniten yhdistetyn portin yleisimmät käyttötarkoitukset. Voidaan nähdä, että Nessus-skannaus on keskittynyt etäkäyttöpalveluiden, tietokantojen ja tiedostojensiirron protokolliin.

Taulukko 6-1.Portit ja niiden palvelut.

Resurssit	Portin käyttö
21/tcp	FTP-ohjauskomennot
23/tcp	Telnet-protokolla
2401/tcp	CVS-versionhallintasysteemi
1433/tcp	MSSQL-palvelin
3389/tcp	Microsoft-päätepalvelin
80/tcp	HTTP-tiedonsiirtoprotokolla
25/tcp	SMTP-sähköpostiprotokolla
1521/tcp	Oracle-tietokanta
22/tcp	SSH Secure Shell
49777/tcp	Xsan Apple-tiedostojärjestelmä

Kuvan 6-3 pylväsdiagrammista nähdään miten tietoliikenne kohdistuu kello 14 ja 15 väliselle ajalle. Skannaus alkoi hieman ennen klo 14, joten voidaan nähdä pieni määrä liikennettä myös siinä. Koska hunajapurkki oli asetettu käyttämättömään osoitteeseen, niin siihen kohdistui suoraan ainoastaan verkkoa skannaavan Nessus-koneen aiheuttama liikenne. Kohdistetun liikenteen lisäksi hunajapurkki havaitsi yleislähetysliikennettä muilta verkossa toimivilta tietokoneilta.



Kuva 6-3. Yhteyksien määrä tunneittain lajiteltuna.

Snort tunkeutumisen havaitsemisjärjestelmä antoi Nessus-skannauksesta viisi hälytystä. Ensimmäisen tunniste on 18753. Se on Mentor ADSL-FR4II reitittimen ohjelmiston haavoittuvuuden hyväksikäyttöyritys. Onnistuessaan se paljastaisi salasanan hyökkääjälle. [25] Toisen ja kolmannen tunniste on 24812. Se on yritys hyväksi käyttää Samsung-tulostinohjelmiston haavoittuvuutta, jolla hyökkääjä voi ottaa laitteen haltuunsa. [28] Neljännen tunniste on 16487. Se on Energizer DUO USB patteri-laturi-ohjelmiston takaoven hyväksikäyttöyritys. Sen avulla olisi mahdollista ladata ohjelmia koneelle ja käynnistää ne. [26] Viides tunniste 15930 on Microsoft Windows-käyttöjärjestelmän haavoittuvuuden hyväksikäyttöyritys. SMB2-protokollan toteutuksessa on virhe, jota hyödyntämällä voidaan aiheuttaa palvelunestohyökkäys. [27] Taulukosta 6-2 nähdään hyökkäyksiin käytetyt portit ja ajankohdat. Hyökkäykset havaittiin muutaman minuutin sisällä toisistaan.

Taulukko 6-2. Snort-hälytykset

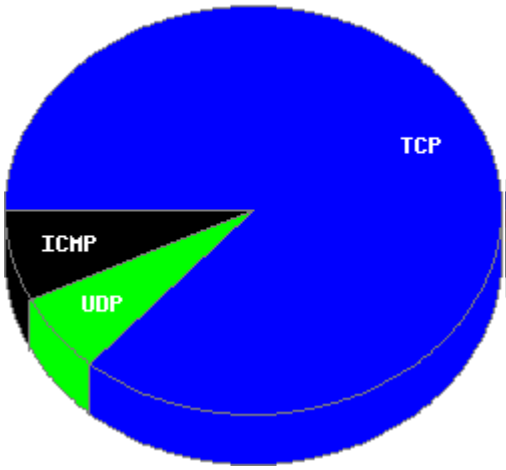
Lähdeosoite	Kohdeosoite	Tunniste	Kellonaika	Portti	Havaintopv.
192.168.0.188	192.168.0.117	18753	14.06	10001	1
192.168.0.188	192.168.0.115	24812	14.07	161	1
192.168.0.188	192.168.0.117	24812	14.07	161	1
192.168.0.188	192.168.0.117	16487	14.07	7777	1
192.168.0.188	192.168.0.117	15930	14.13	445	1

6.2 Laajakaistaverkko

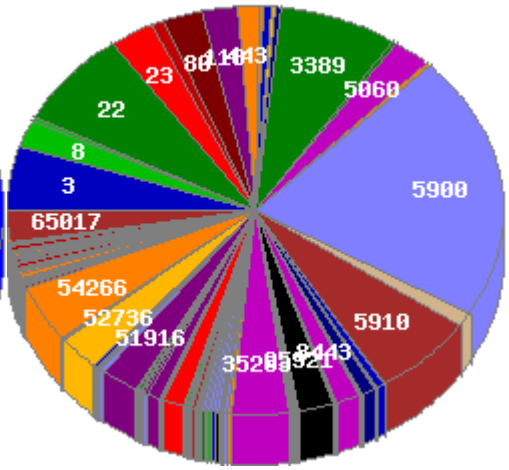
Laajakaistaverkkotapauksessa haluttiin tutkia oman verkon ulkopuolelta tulevia uhkia. Havainnointijärjestelmä asetettiin reitittimen DMZ-alueelle. Tarkastelujakson pituus oli kahdeksan vuorokautta. Tietoa kerättiin hunajapurkkien ja tunkeutumisen havaitsemisjärjestelmän lokitiedostoista.

Tämän havainnointijakson aikana tunkeutumisen havaitsemisjärjestelmä Snortin dynaamisten sääntöjen raja-arvot ylittyivät vain kerran. Hälytyksen tunniste oli 15699. Se viittaa Firefox-selaimen tunnetun haavoittuvuuden hyväksikäyttöyritykseen [22]. Tämän hälytyksen tarkempi tarkastelu osoitti sen olleen väärä hälytys, joka syntyi verkkoon liitetyn siltaavan reitittimen uudelleen käynnistyessä. Se kuormitti verkkoa ylimääräisellä liikenteellä Web-selaimessa avoinna olleeseen reitittimen hallintasivustoon.

Tässä tapauksessa tuli havainnointijakson aikana hunajapurkille yhteensä 2864 yhteyttä. Näistä 2475 kappaletta oli TCP- , 183 kappaletta UDP- ja 206 kappaletta ICMP-yhteyksiä. Kuvasta 6-4 nähdään, miten protokollien määrä jakaantui ja kuvasta 6-5, mihin portteihin liikenne jakaantui.

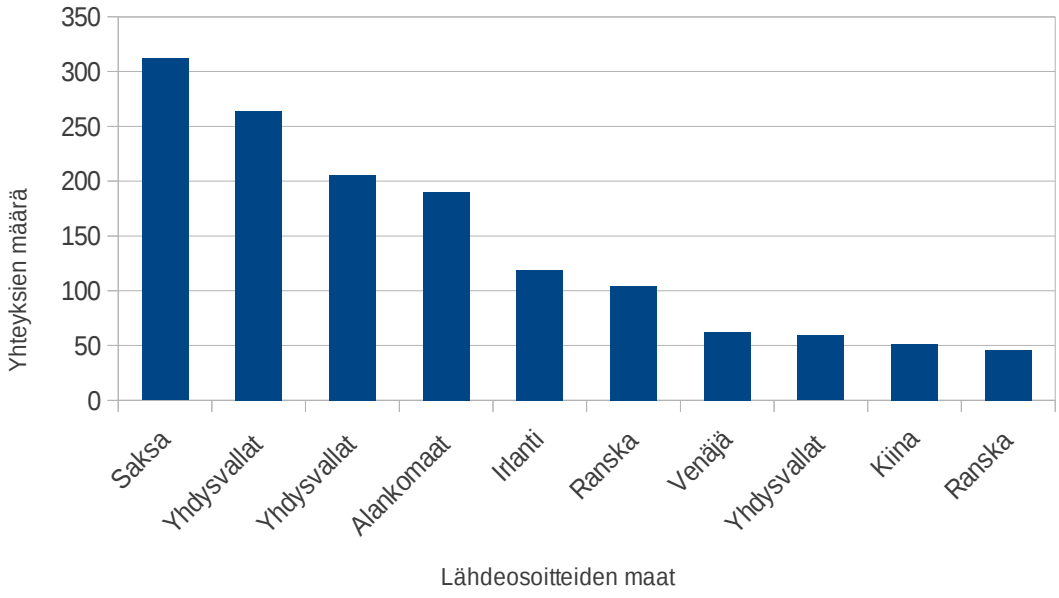


Kuva 6-4. Protokollajakauma.



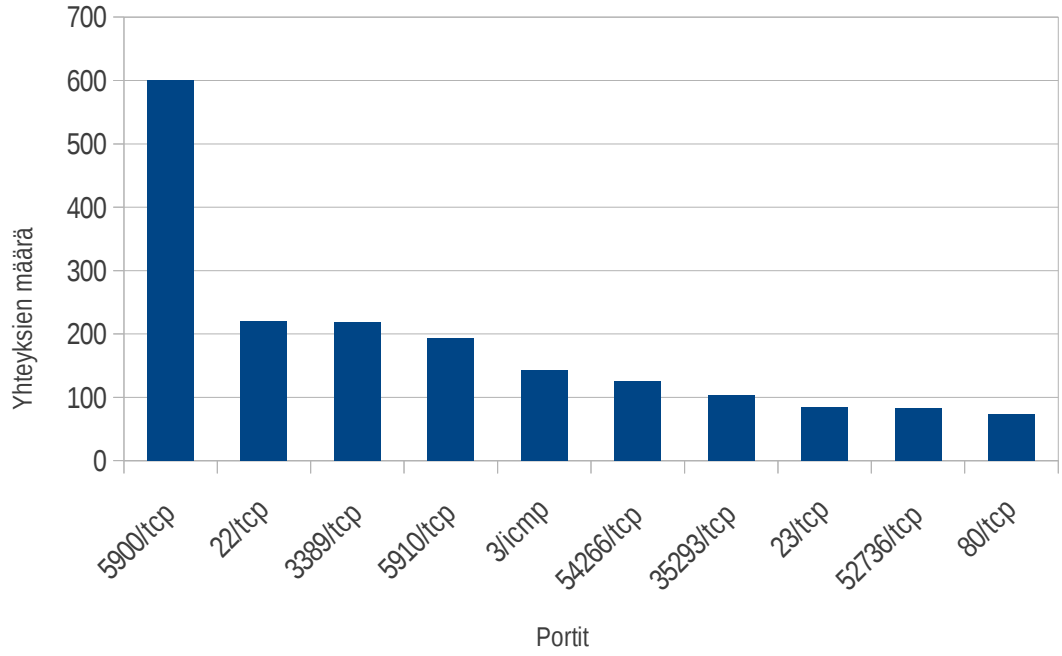
Kuva 6-5. Porttijakauma.

Honeydsum-ohjelmalla on vaikeuksia suurten lokitiedostojen kanssa. Se ei kyennyt tuottamaan kuvaajaa, joka näyttää kaikkien erillisten lähdeosoitteiden yhteyksien määrät. Yhteenvedosta saadaan luotua kuva 6-6, jossa on esiteltynä eniten hunajapurkille yhteydenottoja ottaneiden lähdeosoitteet ja yhteyksien määrät. Lähdeosoitteista yksi ylitti 300 yhteyden määrän, kaksi ylitti 200 yhteyden määrän ja kolme ylitti sadan yhteyden määrän. Nähdään myös lähdeosoitteiden maantieteelliset sijainnit.



Kuva 6-6. Eniten yhdistäneiden lähdeosoitteiden yhteyksien määrät.

Kuvassa 6-7 on esitelty yhteyksien määrä porteittain. Nähdään, että porttiin 5900 on tullut lähes kolminkertainen määrä liikennettä seuraavaksi tulleisiin portteihin 22, 3389 ja 5910 verrattuna.



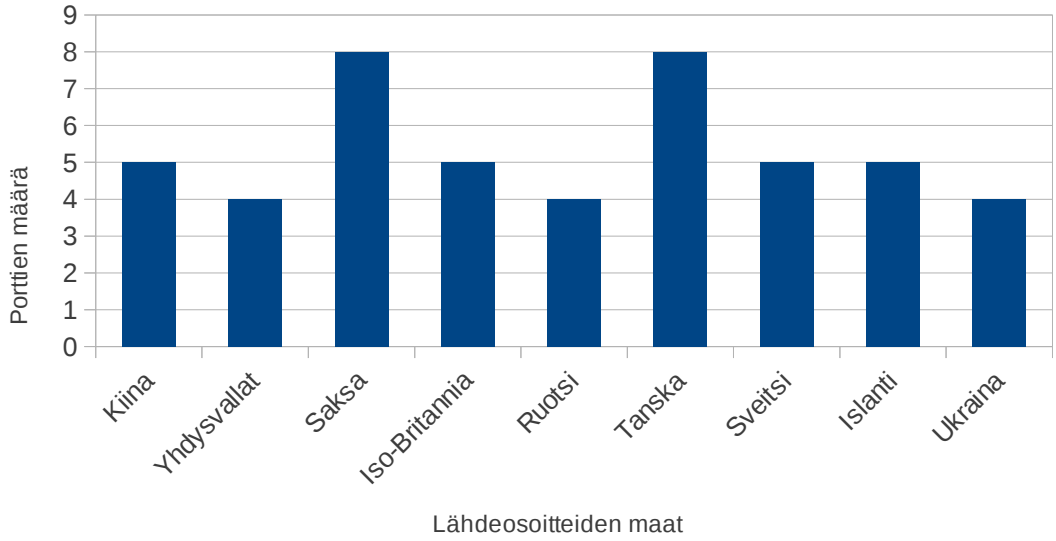
Kuva 6-7. Kymmenen eniten käytettyä porttia.

Taulukossa 6-3 on esitelty kymmenen käytetyimmän portin yleisimmät palvelut. Voidaan nähdä, että etäkäyttö- , etähallinta- ja tiedonsiirtoprotokollat olivat eniten kokeiltujen joukossa. Oletettavasti tarkoituksena oli yrittää saada laitteistoa hallintaan käyttämällä vanhentuneita ohjelmistoversioita ja paikkaamattomia haavoittuvuuksia. Lisäksi havaittiin ICMP-viestejä, joista viestikoodilla 3 oli eniten yhteyksiä. Se merkitsee, että kohde ei ole saavutettavissa. Yhteenvedosta nähdään, että myös viestikoodilla 8 kulkevia viestejä oli verkossa. Se merkitsee Echo-viestiä.

Taulukko 6-3. Käytetyimpien porttien palvelut.

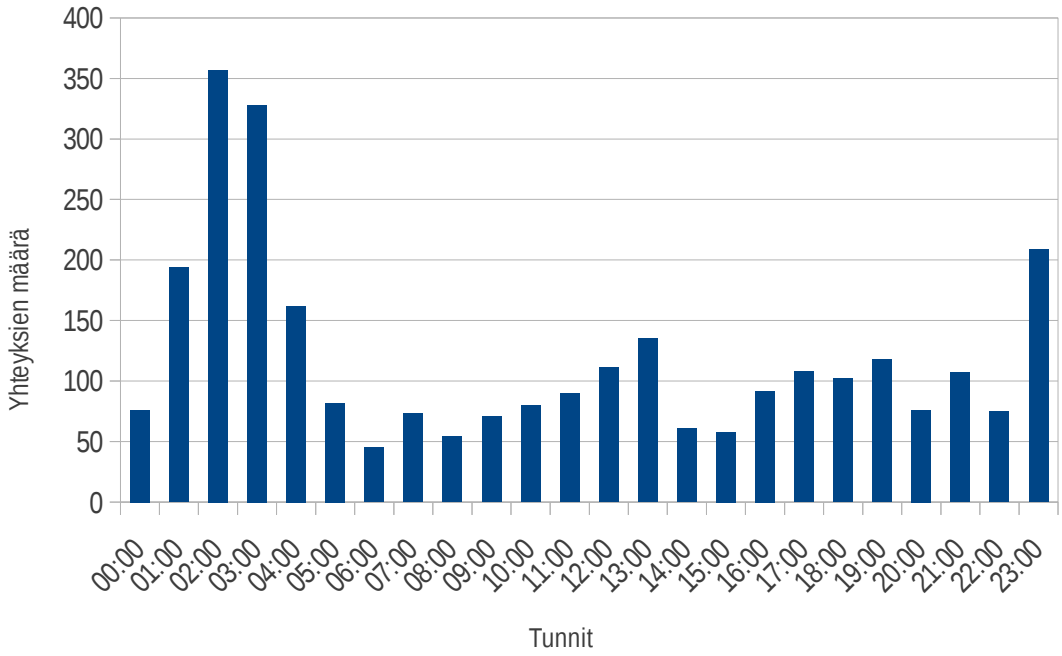
Resurssit	Portin käyttö
5900/tcp	Virtual Network Computing-etäkäyttöprotokolla
22/tcp	SSH Secure Shell
3389/tcp	Microsoft-päätepalvelin
5910/tcp	Context Management, sisällön hallinta
3/icmp	ICMP koodi 3, kohdeosoite saavuttamattomissa
54266/tcp	Xsan Applen tiedostojärjestelmä
3529/tcp	Jboss IIOP/SSL
23/tcp	Telnet-protokolla
52736/tcp	Xsan Applen tiedostojärjestelmä
80/tcp	HTTP-tiedonsiirtoprotokolla

Kuvassa 6-8 on kuvattu kymmenen suurinta porttiskannausta. Niissä yhdestä lähdeosoitteesta oli lähetetty useaan peräkkäiseen tai lähekkäiseen porttiin liikennettä. Voidaan nähdä ettei kyseessä ollut kovin suuria skannauksia. Maista nähdään, että tämän kaltaisia yhteydenottoja on tullut joka puolelta maailmaa. Näistä suurin osa sijoittuu Eurooppaan. Kuva näyttää moneenko porttiin otettiin yhteyttä, mutta se ei kerro kuinka monta kertaa samaan porttiin oltiin yhteydessä.



Kuva 6-8. Porttiskannausten lähdeosoitteet maittain.

Kuvasta 6-9 nähdään miten liikenne on jakaantunut vuorokauden tunneille. Selkeä huippu sijoittuu aamu yhden ja viiden väliin. Kuudelta liikenne määrä on pohjissaan. Myös päivisin yhdeltä sekä yöllä yhdeltätoista on havaittavissa korkeampia liikennemääriä.

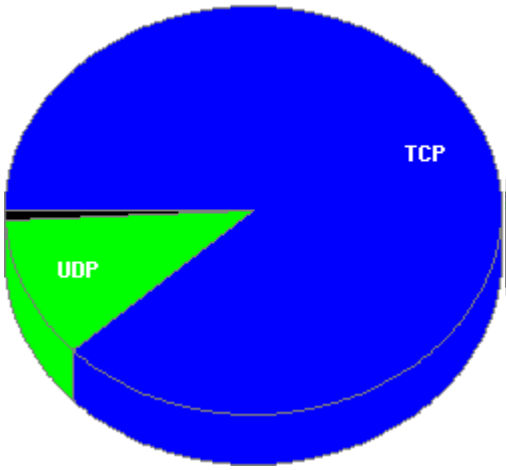


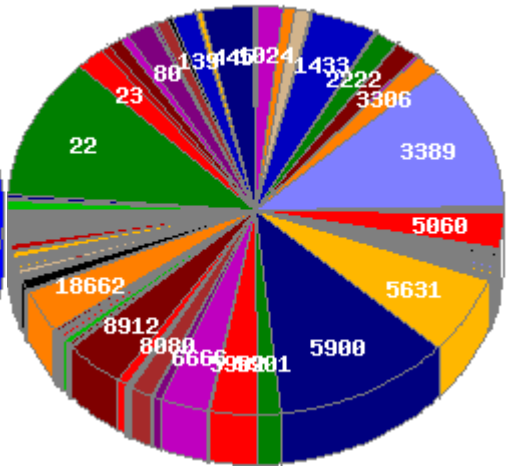
Kuva 6-9. Laajakaistaverkon yhteyksien määrät tunneittain.

6.3 Matkapuhelinverkko

Matkapuhelinverkkotapauksessa havainnoitiin oman verkon ulkopuolelta, matkapuhelinverkosta tapahtuvaa vihamielistä liikennettä suojaamattomaan DMZ-alueen hunajapurkkiin. Tarkastelujakson pituus oli yhdeksän vuorokautta.

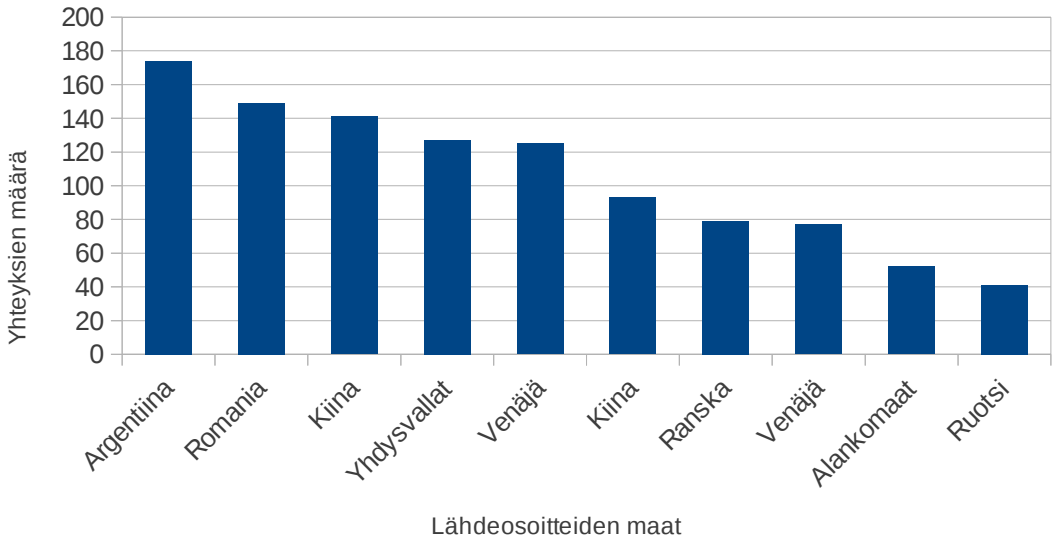
Kuvasta 6-10 voidaan nähdä, että hunajapurkille saapuva liikenne on pääosin TCP-yhteyksiä. Kaikkiaan liikenneyhteyksiä oli 2563 kappaletta. Niistä 2254 kappaletta oli TCP-yhteyksiä, 291 kappaletta oli UDP-yhteyksiä ja 18 kappaletta ICMP-yhteyksiä. Kuvassa 6-11 esitellään kaikki hunajapurkille tulleet yhteydet lajiteltuina portti-numeron mukaan. Voidaan nähdä, että esimerkiksi portteihin 3389, 5900, 22 ja 5631 on tullut paljon yhteyden yrityksiä. Liikennettä tuli yhteensä 581 eri IP-osoitteesta.





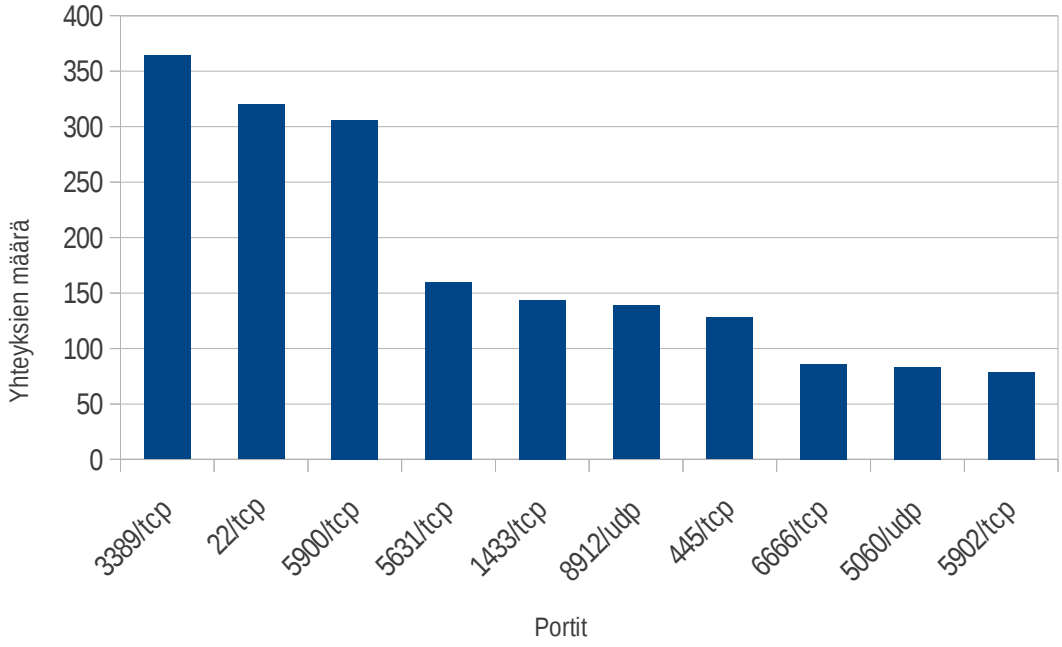
Kuva 6-10. Liikenne protokollittain. *Kuva 6-11. Liikenne porteittain.*

Huomataan, että myös tässä mittauksessa lokitiedoston suuri koko tuottaa Honeydsum-ohjelmalle vaikeuksia. Se ei ole kyennyt tuottamaan kuvaajaa kaikista lähdeosoitteista ja niistä otetuista yhteyksistä. Kuvassa 6-12 on Honeydsum-yhteenvedosta tehty kuvaaja. Siinä esitellään kymmenen vilkkaimmin yhteyksiä ottaneen lähdeosoitteen sijainti ja yhteyksien määrä.



Kuva 6-12. Yhteyksien määrä lähdemaittain jaoteltuna.

Kuvassa 6-13 voidaan nähdä kymmenen eniten liikennöinnissä käytetyn portin yhteysmäärät. Kolme käytetyintä ovat vastaanottaneet selkeästi enemmän yhteyksiä kuin muut.



Kuva 6-13. Yhteyksien määrä porteittain jaoteltuna.

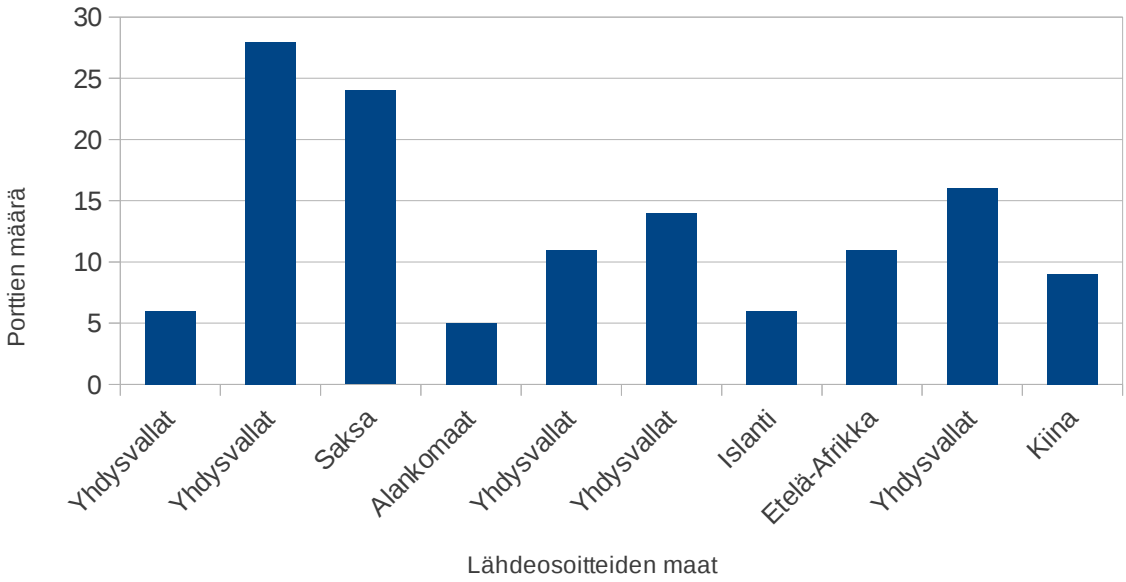
Taulukossa 6-4 esitellään suosituimpien porttien palveluita. Voidaan nähdä, että ne koostuvat enimmäkseen etäkäyttöpalveluista ja tiedostonsiirtopalveluista. Mukana on myös IRC-chat-palvelimen portti ja Microsoftin tietokantapalvelimen portti. Porttiin 18662 ei löytynyt virallisesti eikä epävirallisesti käytössä olevaa palvelua.

Taulukko 6-4. Käytetyimmät portit ja niiden palvelut.

Resurssit	Portin käyttö
3389/tcp	Microsoft-päätepalvelin
5900/tcp	Virtual Network Computing-etäkäyttöprotokolla
22/tcp	SSH Secure Shell
5631/tcp	Symantec pcAnywheredata
1433/tcp	MSSQL-palvelin
8912/udp	Windows Client Backup
445/tcp	Microsoft-tiedostonjako
5902/tcp	Virtual Network Compurter Display: 2
6666/tcp	Internet Relay Chat, IRC
18662/tcp	Käyttämätön

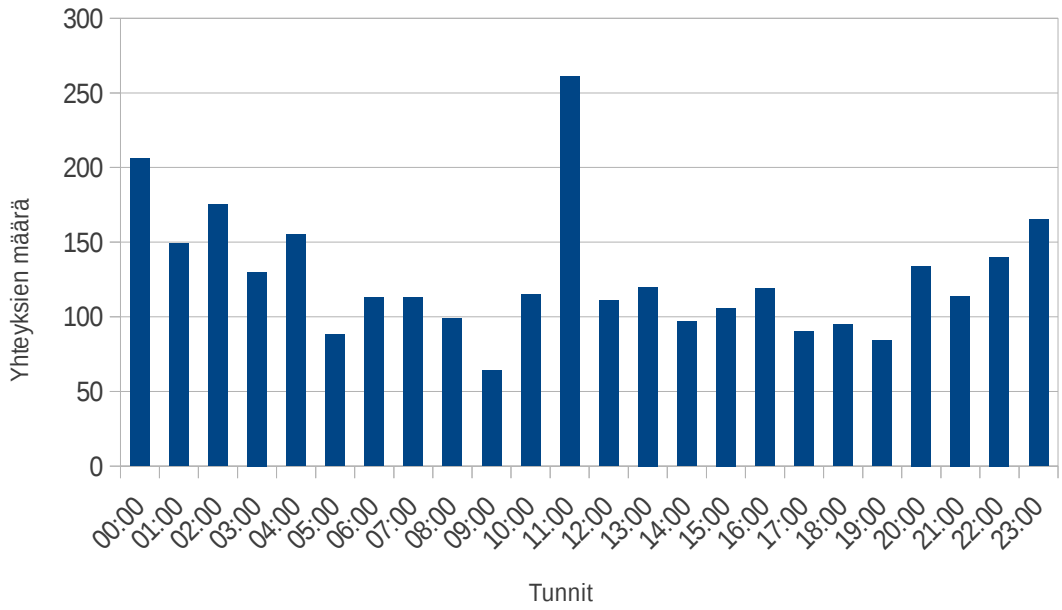
Kuvassa 6-14 esitellään kymmenen suurinta porttiskannausta tehnyttä lähdeosoitetta ja käytettyjen porttien määrä. Nähdään myös niiden maatieteellinen sijainti. Eniten

erillisiä porttiskannauksia on tullut Yhdysvalloista. Kuva esittää moneenko porttiin lähdeosoitteesta on otettu yhteyttä, mutta se ei kerro montako yhteydenottoa tehtiin yksittäiseen porttiin.



Kuva 6-14. Suurimmat porttiskannaukset tehneet lähdeosoitteet.

Kuvassa 6-15 voidaan nähdä miten liikenne sijoittuu vuorokauden tunneille. Nähdään, että liikenteen määrässä on piikit kahdentoista ja yhden välillä yöllä, sekä yhdeltätoista päivällä. Päiväsaikaan liikenne on ollut vähäisempää kuin iltaisin ja määrässä pohjakohdat löytyvät yhdentoista piikin molemmin puolin.



Kuva 6-15. Yhteyksien määrät jaoteltuna vuorokauden tunneille.

Snort tunkeutumisen havaitsemisjärjestelmä antoi havaintojakson aikana yhteensä yksitoista hälytystä. Ne on listattu taulukossa 6-5. Näistä oli viisi tunnisteeltaan 9423, kuusi oli tunnisteeltaan 3397. Ensimmäinen tunniste ilmoittaa mahdollisen Lovegate nimisen madon taikka viruksen läsnäolosta havaintoverkossa [23]. Toinen ilmoittaa yrityksestä käyttää hyväksi Microsoft RPC DCOM-palvelun tunnettua haavoittuvuutta [24]. Palvelua käytetään tietokoneen etäkäytössä.

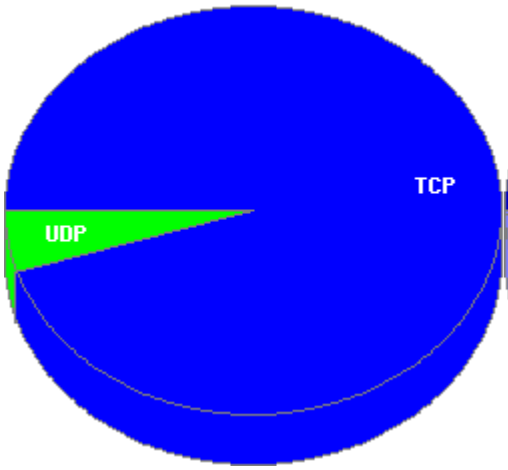
Taulukko 6-5. Snort-hälytykset.

Lähdeosoite	Tunniste	Kellonaika	Portti	Havaintopv	Lähdemaa
A	9423	2.46	135	1	Saksa
A	3397	2.46	135	1	Saksa
B	9423	7.5	135	2	Saksa
B	3397	7.5	135	2	Saksa
C	9423	8.36	135	3	Saksa
C	3397	8.36	135	3	Saksa
D	3397	10.32	135	6	Saksa
E	9423	20.15	135	7	Saksa
E	3397	20.15	135	7	Saksa
F	9423	1.28	135	8	Saksa
F	3397	1.28	135	8	Saksa

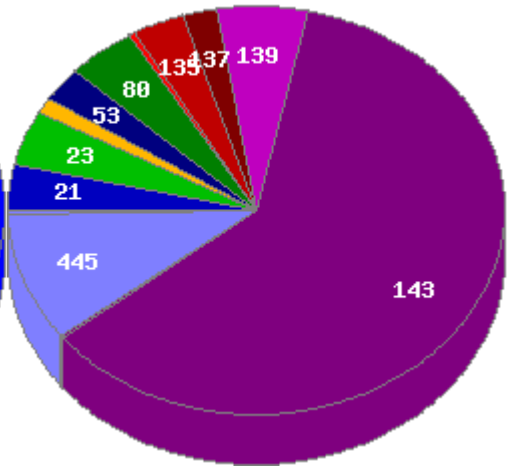
6.4 Virtuaalipalvelin

Tässä tapauksessa matkapuhelinverkosta hunajapurkkiin pääsevää liikennettä oli rajoitettu ohjaamalla sille ainoastaan reitittimen virtuaalipalvelimelle määritellyt yhteydet. Haluttiin jäljitellä Internetiin yhdistetyn sisäverkon tilannetta. Tapauksen havainnointijakson pituus oli kuusi vuorokautta.

Kuvasta 6-16 nähdään, että tietoliikenne ollut suurimmaksi osaksi TCP-yhteyksiä, vähän UDP-yhteyksiä eikä ollenkaan ICMP-yhteyksiä. Tätä voidaan odottaa, sillä TCP-protokolla on käytetyin yhteysprotokolla. Kaiken kaikkiaan yhteyksiä oli 740. Niistä TCP-yhteyksiä oli 704 ja UDP-yhteyksiä oli 36. Kuvan 6-17 kuvaajassa esitetyssä hunajapurkille tulleesta liikenteestä on porttiin 143 suuntautunut selkeästi suurin osa.

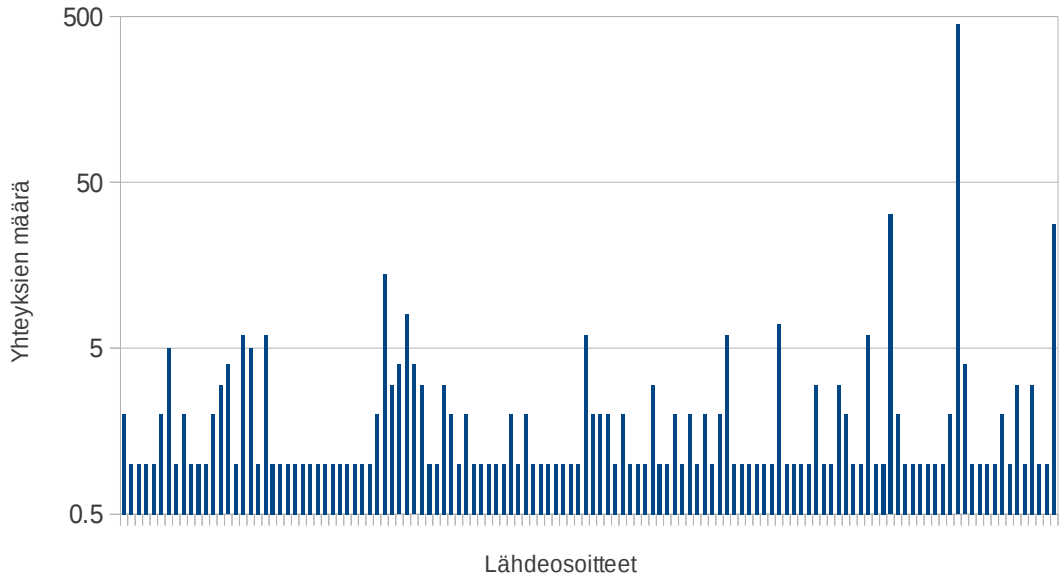


Kuva 6-16. Liikenne protokollittain.



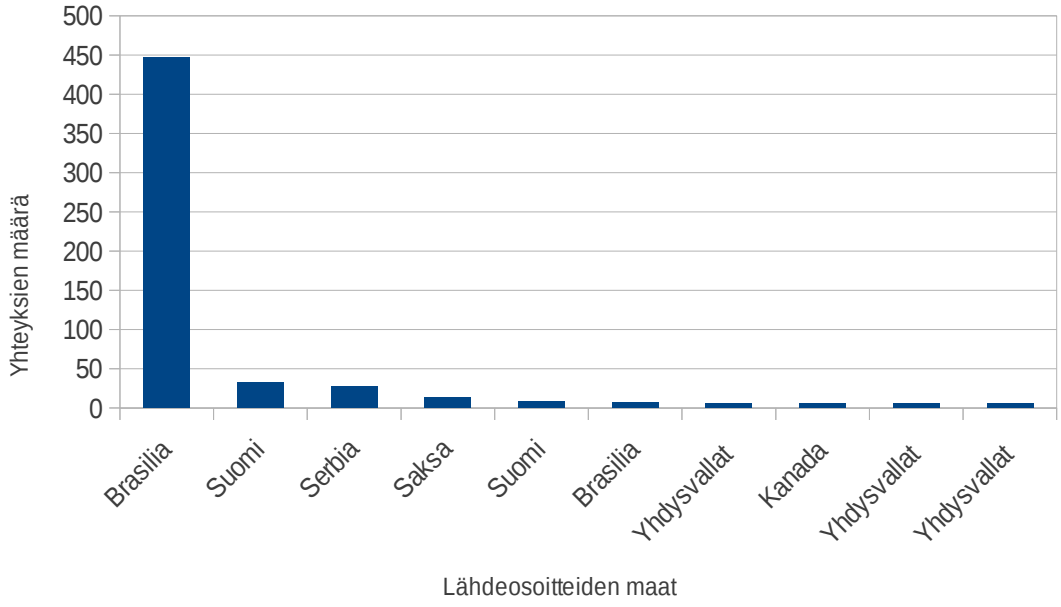
Kuva 6-17. Liikenne porteittain.

Kuva 6-18 esittää yhteyksien määrää lähdeosoitteittain lajiteltuina. Nähdään, että kuvaajassa on yksi suuri piikki. Siinä on yhdeltä lähdeosoitteelta tehty 446 yhteydenottoa. Lähdeosoite taulukosta nähdään, että kyseessä on yhdestä osoitteesta porttiin 143 osoitetuista TCP-yhteyksistä. Havainnointijakson aikana hunajapurkkiin tuli 740 yhteyttä 126:sta eri lähdeosoitteesta ja ne käyttivät 13:sta eri portti-protokolla-yhdistelmää.



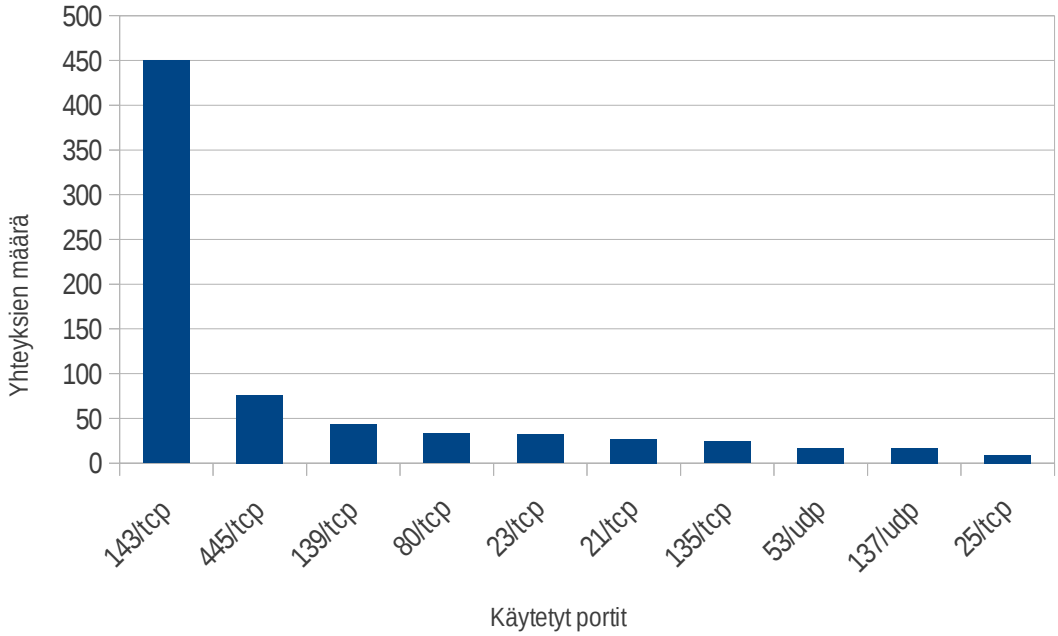
Kuva 6-18. Lähdeosoitekohtainen yhteyksien määrä.

Kuvassa 6-19 on esitelty kymmenen eniten yhteyksiä ottaneiden lähdeosoitteiden yhteysmäärät. Aikaisemmin mainitusta osoitteesta tulleen liikenteen määrässä on selkeä ero muihin.



Kuva 6-19. Kymmenen vilkkaimman lähdeosoitteen yhteyksien määrät.

Kuvassa 6-20 esitellään eniten käytetyt portit. Portti 143 on selkeästi saanut eniten yhteydenottoja. Taulukosta nähdään, että seuraavaksi eniten on otettu yhteyttä 445 porttiin ja siitä seuraaviin portteihin tasaisesti laskevin määrin. Tästä nähdään, että portit joissa on yleisimmin palveluita, ovat myös niitä, joihin liikenne kohdistuu.



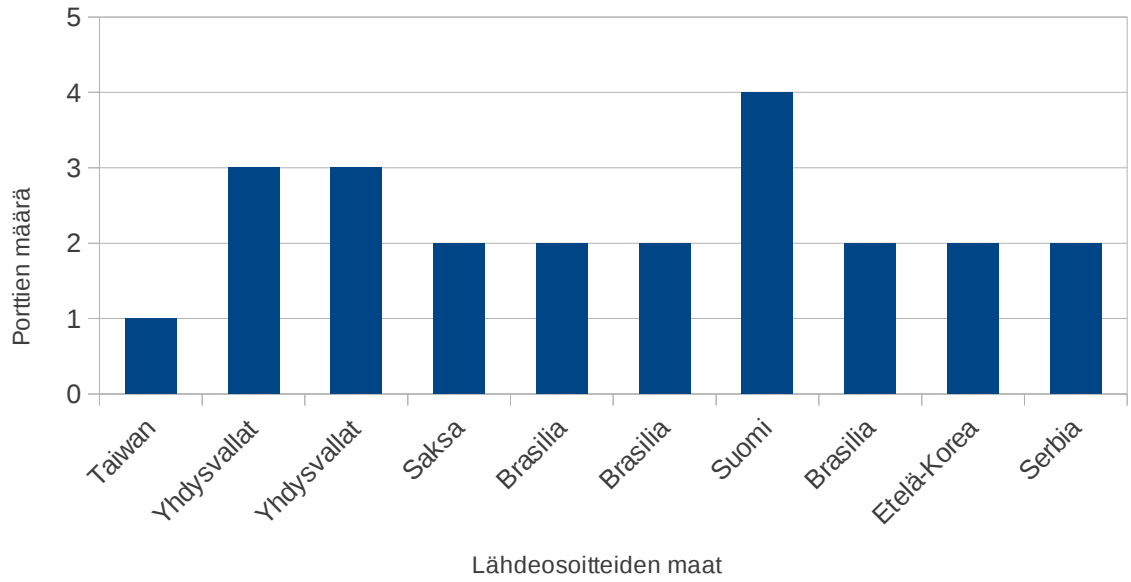
Kuva 6-20. Kymmenen käytetyintä porttia.

Taulukossa 6-6 on esitelty kymmenen yleisimmän portin tavallisimmat palvelut. Nähdään, että liikennettä on tullut etähallinta- , tiedonsiirto- ja sähköpostipalveluihin. Erityisesti IMAP-sähköpostiprotokollalle on tullut yhteyksiä.

Taulukko 6-6. Käytetyimmät portit ja niiden palvelut.

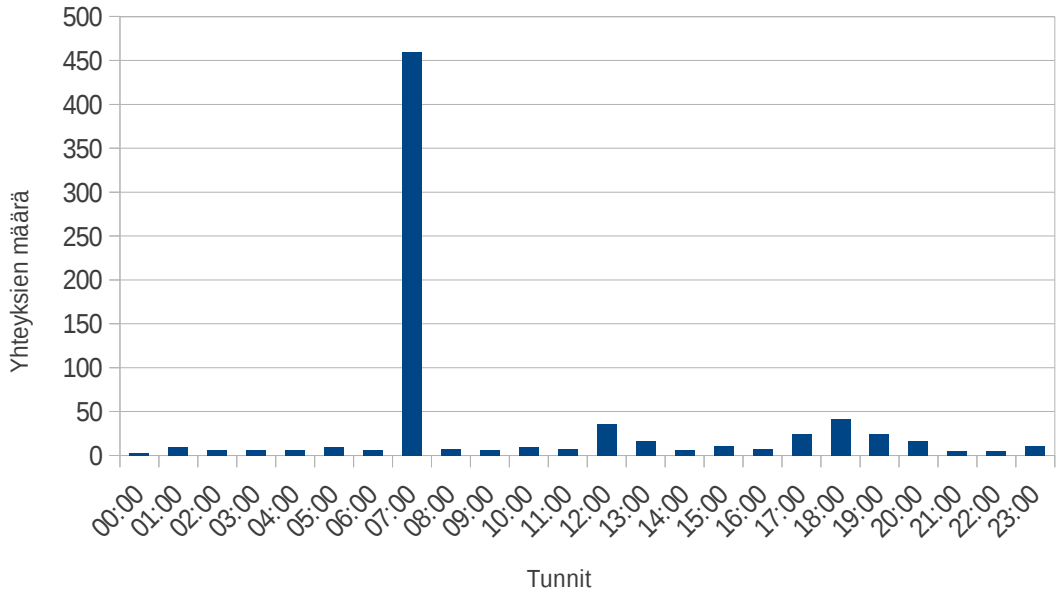
Resurssit	Portin käyttö
143/tcp	IMAP-sähköpostiprotokolla
445/tcp	Microsoft-tiedostonjako
139/tcp	NetBIOS-istuntopalvelu
80/tcp	HTTP-tiedonsiirtoprotokolla
23/tcp	Telnet-protokolla
21/tcp	FTP-palvelun ohjauskomennot
135/tcp	Microsoft EPMAP, palveluiden etähallinta
53/udp	DNS, Domain Name System
137/tcp	NetBIOS-nimipalvelu
25/tcp	SMTP-sähköpostiprotokolla

Kuvassa 6-21 on esitelty suurimmat porttiskannaukset ja niissä käytettyjen porttien määrät. Lähdeosoitteista on esitelty niiden maantieteellinen sijainti. Nähdään, että useita portteja läpikäyviä skannauksia oli vain muutama. Se esittää moneenko porttiin on otettu yhteyttä, mutta ei kerro montako yhteydenottoa tehtiin yhteen porttiin.



Kuva 6-21. Porttiskannausten lähdeosoitteet ja käytettyjen porttien määrä.

Kuvasta 6-22 nähdään miten liikennöinti sijoittuu vuorokauden tunneille. Nähdään selkeästi, että kello 7:n ja 8:n välillä on valtava piikki yhteydenottojen määrässä. 460 yhteyttä tunnin sisällä, kun normaali näyttää olevan kuuden ja yhdentoista yhteyden välillä. Myös kello 12:n aikaan ja kello 17:n ja 21:n välillä on selkeät piikit.



Kuva 6-22. Yhteyksien määrä vuorokauden tunneille jaoteltuna.

Havainnointijakson aikana Snort hälytti kaksitoista kertaa. Kuusi hälytyksistä oli tunnisteella 9423 ja toiset kuusi oli tunnisteella 3397. Taulukosta 6-7 nähdään ajankohta, kohdeportti ja lähdeosoitetta korvaava kirjain. Tämän perusteella nähdään, että yhdestä osoitteesta tehdään samanaikaisesti kaksi hyökkäystä.

Taulukko 6-7. Snort-hälytykset.

Lähdeosoite	Tunniste	Kellonaika	Portti	Havaintopv	Lähdemaa
A	9423	13.54	135	4	Suomi
A	3397	13.54	135	4	Suomi
B	9423	15.22	135	4	Suomi
B	3397	15.22	135	4	Suomi
B	9423	13.22	135	5	Suomi
B	3397	13.22	135	5	Suomi
C	3397	19.04	135	5	Suomi
C	9423	19.04	135	5	Suomi
D	3397	20.21	135	5	Saksa
D	9423	20.21	135	5	Saksa
E	3397	7.27	135	6	Saksa
E	9423	7.27	135	6	Saksa

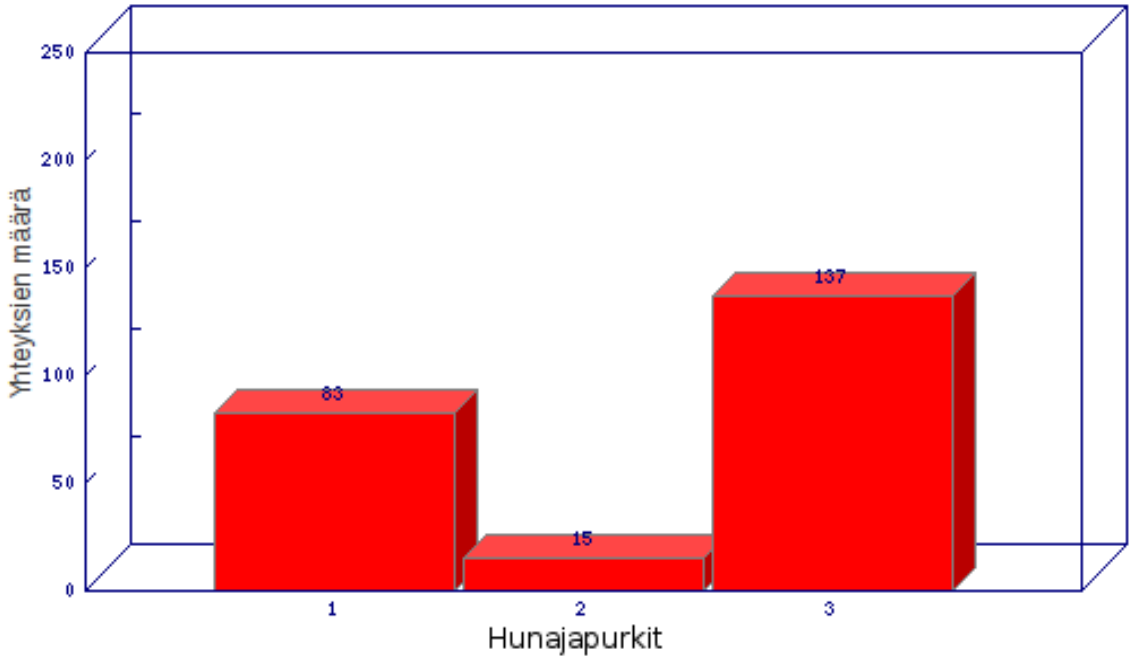
6.5 Hunajaverkko

Hunajaverkkotapauksessa haluttiin testata miten hyvin Honeydsum-ohjelma kykenee esittämään usean hunajapurkin lokitiedoston graafisesti. Tahdottiin myös tarkastella

minkälaista liikennettä erilaisille käyttöjärjestelmille saapuu. Tarkastelujakson pituus oli yksitoista päivää. Hunajaverkossa tietokoneet ovat reitittimen palomuurilla suojatussa verkossa, jonne virtuaalipalvelimella ohjataan matkapuhelinverkosta saapuvaa liikennettä. Tämä tarkoittaa, että sinne ohjautuva liikenne kohdistuu itse määriteltyihin portteihin ja palveluihin, kuten tavallisessa suojatussa sisäverkossa.

Havainnointijakson aikana tunkeutumisen havaitsemisjärjestelmä Snort tunnisti hyökkäyksiä hunajapurkissa 192.168.1.111. Siinä sijaitsi Windows 2000-palvelin hunajapurkki. Toisille hunajapurkeille ei tullut Snort-hälytystä aiheuttanutta liikennettä.

Kuvassa 6-23 on yhteyksien määrä esitetty hunajapurkkikohtaisesti. Siitä nähdään, että kolmanteen hunajapurkkiin on otettu eniten useimmiten yhteyttä. Sen jälkeen ensimmäiseen ja vähiten toiseen. Kuvassa hunajapurkit ovat 1. Windows 2000 Server osoitteessa 192.168.1.111, 2. Linux 2.4.20 osoitteessa 192.168.1.112 ja 3. Cisco 2500-reititin osoitteessa 192.168.1.113. Liikenne hunajapurkkeihin koostui kokonaan TCP yhteyksistä.

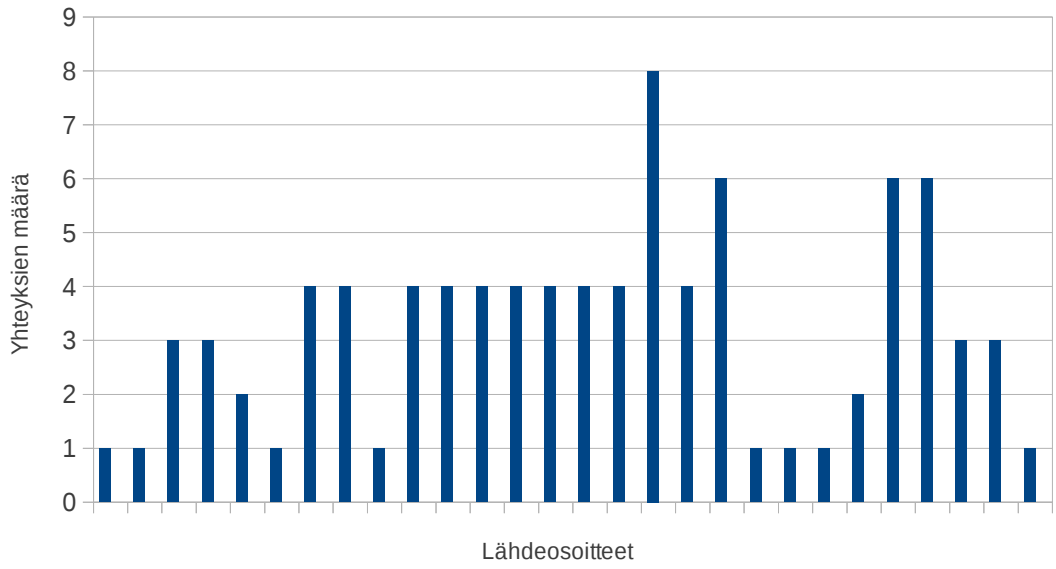


Kuva 6-23. Honeydsum-yhteenveto yhteyksien määrästä hunajapurkeittain.

Windows 2000 Server-hunajapurkki

Windows 2000 Server-hunajapurkille liikenne ohjautui avoimiin portteihin 135, 137 ja 139, sekä ISS-palvelua jäljittelevälle 80 porttiin. Portiin 137 tuli eniten liikennettä, vaikka se oli vain määritelty avoimeksi eikä siinä ollut asetettuna mitään palvelua.

Kuvassa 6-24 esitellään lähdeosoitekohtainen liikenteen määrä. Nähdään, että lähes kaikissa tapauksissa yhdestä osoitteesta on otettu yhteyttä vain yhteen porttiin. Kolmannessa pylväässä nähdään eroa muihin. Siinä on samasta osoitteesta otettu yhteyttä sekä 80 että 139 portteihin. Yhteensä yhteyksiä hunajapurkille tuli 83 kappaletta 26 eri lähdeosoitteesta.



Kuva 6-24. Windows 2000 Server-hunajapurkin yhteydet lähdeosoiteittain jaoteltuna.

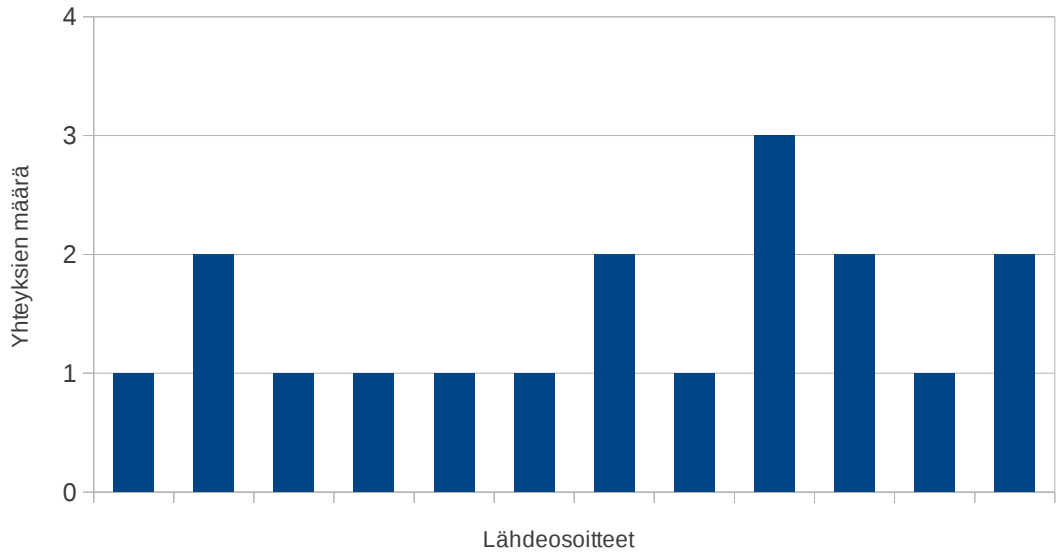
Snort tunnisti havainnointijaksolla kaksikymmentäneljä hyökkäystä. Niistä kaksitoista oli 9423 tunnisteella ja toiset kaksitoista oli 3397 tunnisteella. Snort-hälytykset kohdistuivat Windows 2000 Server-palvelinhunajapurkkiin osoitteessa 192.168.1.111. Taulukossa 6-8 on hyökkäysten ajankohdat, portit ja osoitteita korvaavat kirjaimet. Havaintojakson Snort-hälytysten huippu on ollut kuudentena vuorokautena.

Taulukko 6-8. Snort-hälytykset.

Lähdeosoite	Tunniste	Kellonaika	Portti	Havaintopv	Lähdemaa
A	9423	9.13	135	5	Puola
A	3397	9.13	135	5	Puola
B	9423	17.26	135	6	Belgia
B	3397	17.26	135	6	Belgia
C	9423	18.27	135	6	Espanja
C	3397	18.27	135	6	Espanja
D	9423	21.12	135	6	Espanja
D	3397	21.12	135	6	Espanja
E	9423	10.21	135	6	Unkari
E	3397	10.21	135	6	Unkari
F	9423	10.5	135	6	Romania
F	3397	10.5	135	6	Romania
G	9423	12.15	135	6	Saksa
G	3397	12.15	135	6	Saksa
H	9423	16.37	135	6	Saksa
H	3397	16.37	135	6	Saksa
I	9423	22.24	135	7	Itävalta
I	3397	22.24	135	7	Itävalta
I	9423	3.06	135	7	Itävalta
I	3397	3.06	135	7	Itävalta
J	9423	19.32	135	9	Puola
J	3397	19.32	135	9	Puola
K	9423	21.37	135	9	Turkki
K	3397	21.37	135	9	Turkki

Linux 2.4.20-hunajapurkki

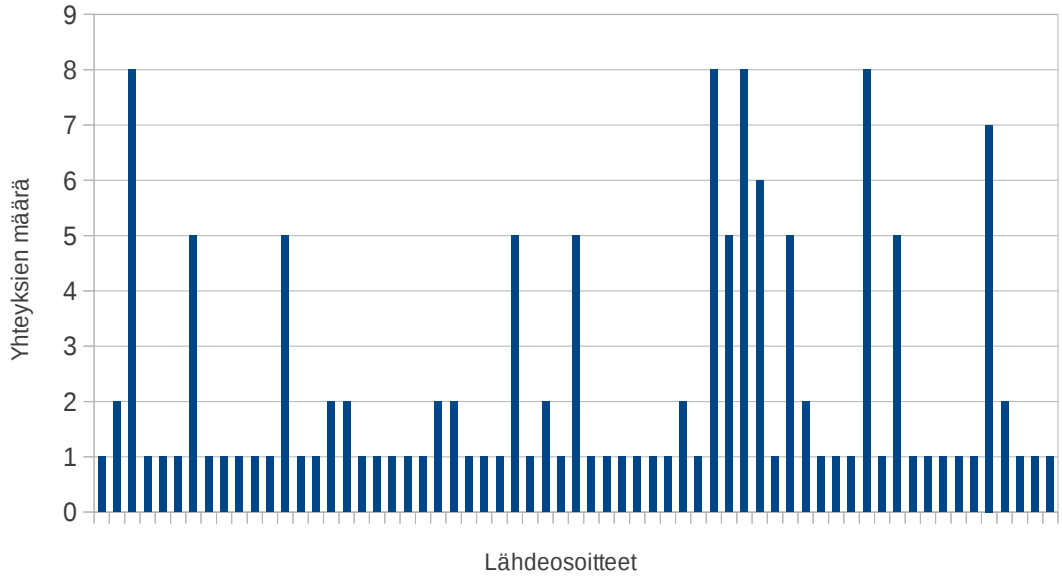
Linux 2.4.20-hunajapurkkiin oli asetettu yksi avoin portti 445 ja kolme porttia asetettiin jäljittelemään palveluita. Portti 21 asetettiin jäljittelemään FTP-palvelua, portti 25 asetettiin jäljittelemään SMTP-palvelua ja portti 110 asetettiin jäljittelemään POP3-palvelua. Huomataan Honeydsum-yhteenvedosta, ettei porttiin 445 tullut ollenkaan liikennettä. Kuvasta 6-25 nähdään, ettei tälle hunajapurkille tullut kovin paljoa liikennettä. Yhteydenottoja oli vain yksi tai kaksi jokaista lähdeosoitetta kohden. Yhteensä yhteyksiä hunajapurkille tuli 15 kappaletta 11 eri lähdeosoitteesta.



Kuva 6-25. Linux-hunajapurkin yhteyksien määrä lähdeosoitteittan.

Cisco-reititin-hunajapurkki

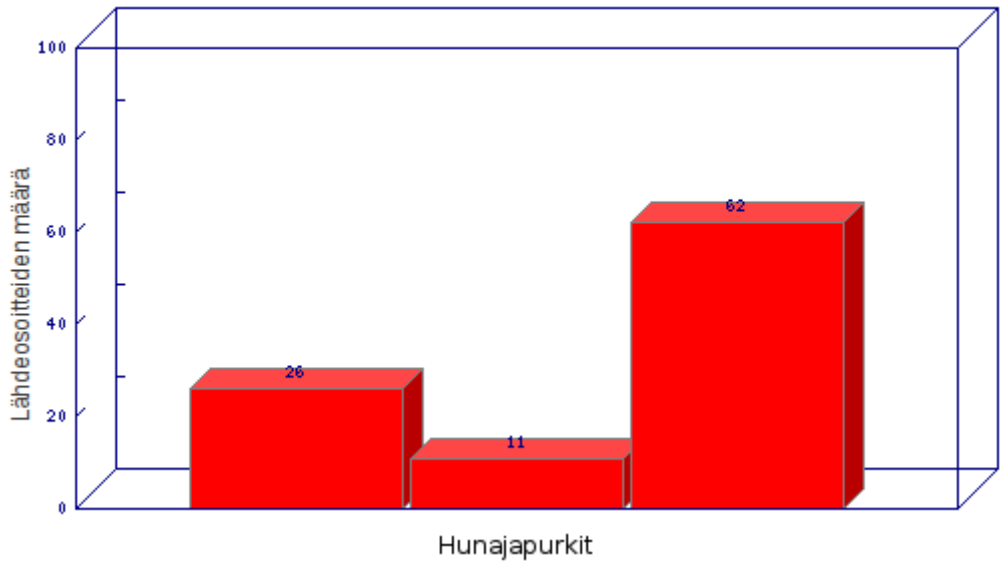
Cisco-reititin-hunajapurkin portti 23 asetettiin jäljittelemään reitittimen telnet-palvelua. Muita portteja sille ei määritelty. Tähän hunajapurkkiin saapui eniten liikennettä ja suurimmasta määrästä lähdeosoitteita. Hunajapurkkiin saapui vain yhteen porttiin suuntautunutta liikennettä. Tämä johtuu siitä, että virtuaalipalvelin ohjasi hunajapurkille ainoastaan määritellyn liikenteen. Yhteensä yhteyksiä hunajapurkille tuli 137 kappaletta 62 eri lähdeosoitteesta. Kuvassa 6-26 nähdään selvää vaihtelua eri osoitteista tulleen liikenteen välillä.



Kuva 6-26. Cisco-reititin-hunajapurkin yhteyksien määrä lähdeosoitteittain.

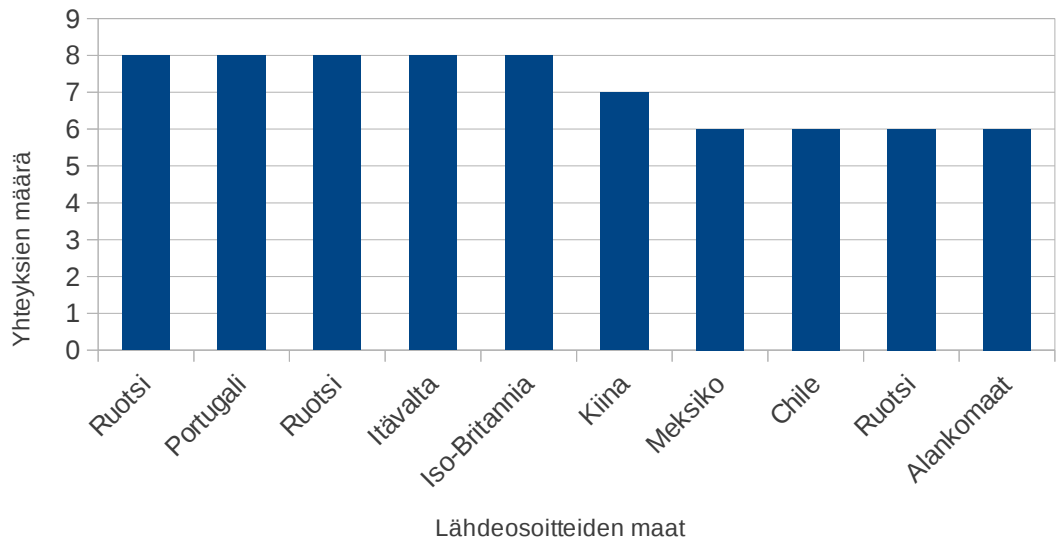
Hunajaverkon yleistietoja

Kuvan 6-27 kuvaajassa näkyy miten erillisten lähdeosoitteiden yhteydenotot jakaantuvat hunajapurkeille. Nähdään, että se muistuttaa aikaisempaa kuvaa 6-23 yhteyksien määrästä. Ne eroaisivat toisistaan mikäli johonkin hunajapurkkiin olisi tullut yhdestä lähdeosoitteesta suuri määrä liikennettä, kuten sisäverkkotapauksen haavoittuvuusskannauksessa.



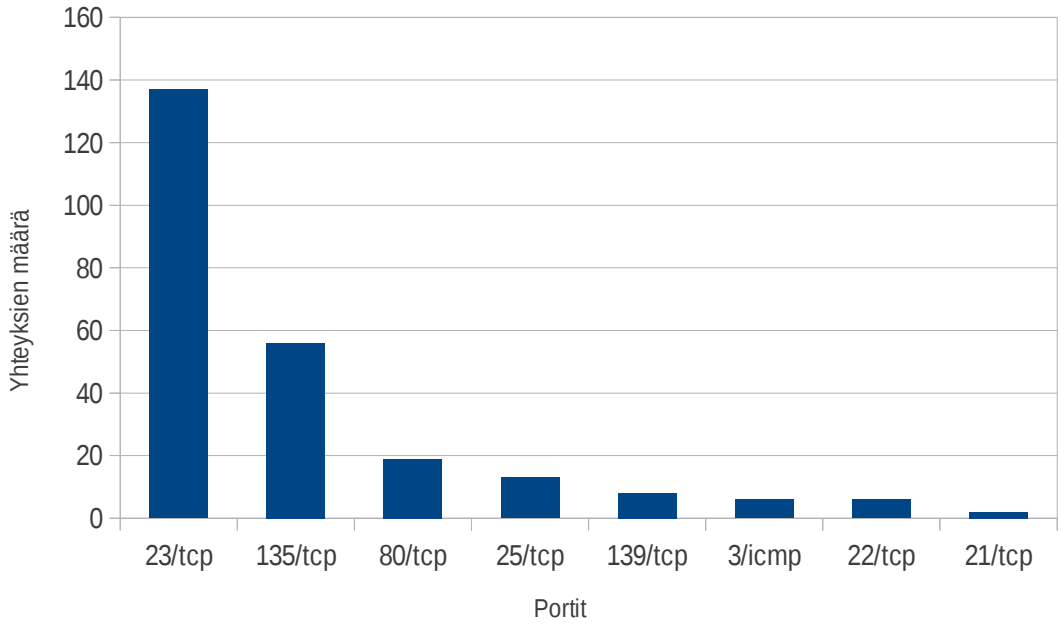
Kuva 6-27. Honeydsum-yhteenveto lähdeosoitteiden määrästä hunajapurkeittain.

Kuvassa 6-28 esitellään kymmenen villkaimman lähdeosoitteen yhteysmäärät ja maatieteellinen sijainti. Nähdään, ettei yksittäisillä osoitteilta tullut suuria määriä yhteyksiä. Maantieteellinen sijainti näyttää, että liikennettä on tullut joka puolelta maailmaa.



Kuva 6-28. Kymmenen villkainta lähdeosoitetta ja niiden yhteyksien määrä.

Kaikkiin hunajapurkkeihin kohdistuneesta liikenteestä suurin osa oli porttiin 23 kohdistuvia TCP-yhteyksiä. Kuvasta 6-29 nähdään, että niitä on selvästi enemmän kuin muita. Siinä portissa jäljitellään reitittimen telnet-palvelinta.



Kuva 6-29. Käytetyimmät portit ja yhteyksien määrät.

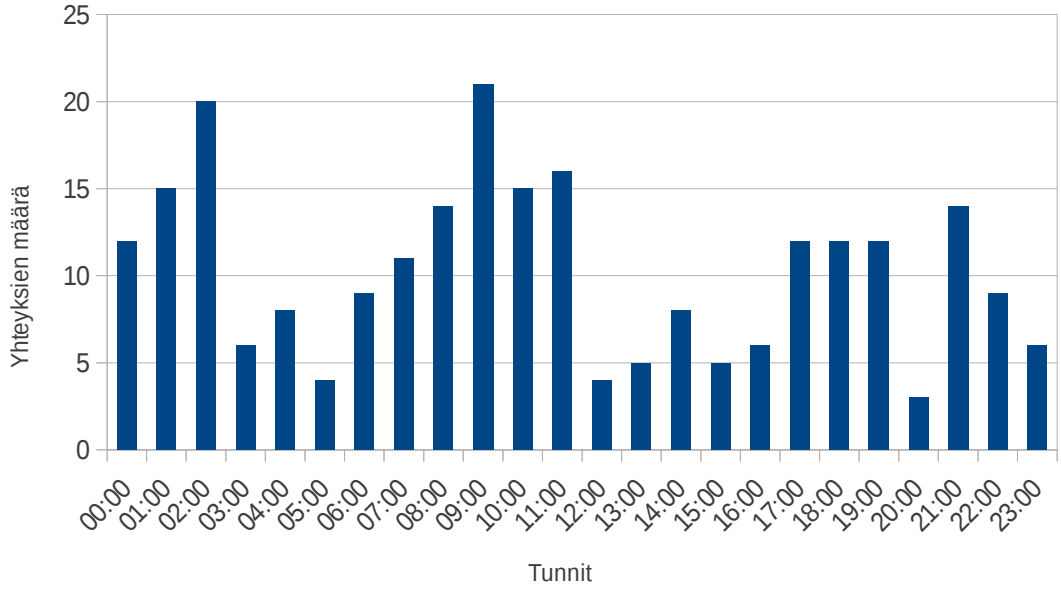
Taulukossa 6-9 on esitelty portit joihin on otettu eniten yhteyksiä ja niissä yleisimmin sijaitsevat palvelut. Tässä tapauksessa näihin portteihin oli virtuaalipalvelimella määritelty reitit. Reititin-hunajapurkille oli porttiin 23 asetettu reitittimen telnet-palvelua jäljittelevä ohjelma.

Taulukko 6-9. Käytetyimmät portit ja niiden palvelut.

Resurssit	Portin käyttö
23/tcp	Telnet-protokolla
135/tcp	Microsoft EPMAP, palveluiden etähallinta
80/tcp	HTTP-tiedonsiirtoprotokolla
25/tcp	SMTP-sähköpostiprotokolla
139/tcp	NetBIOS-istuntopalvelu
21/tcp	FTP-palvelun ohjauskomennot

Kuvasta 6-30 voidaan nähdä miten tietoliikenne jakaantuu vuorokauden tunneille. Suurin osa yhteydenotoista on tapahtunut yöllä ja aamulla, sekä iltapäivällä

vuorotunneille hajaantuneesti, muodostaen kuvaajan piikit. Yhdentoista päivän havainnointijaksosta ei kuitenkaan voida vetää tilastollisia johtopäätöksiä. Liikenteen voi aiheuttaa joukko automatisoituja tietokoneita, jotka satunnaisesti etsivät Internetistä hyökkäyksille alttiita laitteita.



Kuva 6-30. Yhteyksien jakautuminen vuorokauden tunneille.

6.6 Tuotetun tiedon havainnollisuus

Honeydsum-ohjelmistolla tuotetut yhteenvedot antavat yleiskuvan hunajapurkkeihin kulkeneen liikenteen määristä ja laadusta. Kuvaajista kyetään näkemään liikenteessä olleita piikkejä ja erottamaan lähdeosoitteitta, joista on tullut paljon liikennettä. Voidaan tarkastella ajallisesti vuorokauden tunneille jakaantunutta liikennettä, mutta esimerkiksi koko havaintojakson kokoinen ajallinen erittely parantaisi liikenne määrien tulkitsemista. Lisäksi lähdeosoitekohtainen ajallinen tarkastelu helpottaisi siltä saapuneen liikenteen tarkastelua.

Kun lähdeosoitteita on paljon, alkaa niistä luotujen kuvaajien laatu heikkenemään, sillä pylväitä ei enää voi kunnolla erottaa toisistaan. Ratkaisuna voisi olla tarkasteltavan joukon jakaminen useampaan pienempään pylväskuvaajaan. Lisäksi voidaan käyttää Honeydsum-ohjelmiston tuottamaa tekstipohjaista yhteenvetoa kuvaajien tuottamiseen esimerkiksi taulukkolaskentaohjelmalla.

Snort Report antaa tietonsa pääosin taulukoina. Se antaa rajata tiedot haluttuun ajankohtaan, mutta tämä ominaisuus on rajoittunut vain uudempien tapahtumien

tarkasteluun. Vanhojen tapahtumien tarkasteluun voidaan käyttää vain koko ajalta tapahtuneiden hälytysten tarkastelua. Hyökkäysten sisältöä voidaan tarkastella teksti- tai heksadesimaalimuodossa. Niistä kerrotaan kohde ja lähdeosoitteet sekä maantieteellinen sijainti. Hyökkäysten esitys on selkeä, mutta se ei tarjoa tarpeeksi tilastollisia esityksiä ja yhteenvetoja ollakseen tehokas.

Snort Report ja Honeydsum tuottavat tarpeeksi tietoa helpottaakseen tietoliikenteen tutkimista, mutta ne voisivat olla tehokkaampia ja monipuolisempia tiedon tuottamisessa. Summattu tieto on kätevää, koska siitä voi luoda omia kuvaajia tarpeen mukaan, mutta sen tuottamiseksi ohjelmien pitäisi antaa enemmän mahdollisuuksia vaikuttaa sen sisältöön.

6.7 Tulosten analysointi

Toteutettiin viisi verkkotapausta, joissa jokaisessa hunajapurkki ja tunkeutumisen havaitsemisjärjestelmä asetettiin eri sijaintiin. Tässä pohditaan edellä esitettyjä tuloksia.

Sisäverkko

Sisäverkkotapauksessa pyrittiin jäljittelemään verkon sisäistä tietoturvauhkaa suorittamalla Nessus-haavoittuvuusskannaus. Kuvasta 6-2 voidaan nähdä hyökkäyksessä eniten käytetyt portit. Nähdään, että yhteyksien määrä putoaa tasaisesti eri porttien kohdalla. Tämä voi johtua Nessus-haavoittuvuusskannauksen ominaisuuksista. Skannatessaan se on ensin kartoittanut kohteen avoimet portit ja ryhtynyt sitten kokeilemaan hyökkäyksiä.

Taulukossa 6-1 on kerrottu eniten käytettyjen porttien yleisimmät oletuspalvelut. Tarkastellaan hunajapurkkien asetuksia ja käytetyimpien porttien taulukkoa. Viisi kymmenestä portista on yhteneviä. Tämä voi tarkoittaa, että Nessus on skannatessaan huomioinut ne ja määritellyt niitä hyökkäyksen kohteeksi. Nämä portit ovat yleisten palveluiden oletusportteja, joten on uskottavaa, että hyökkääjä keskittyisi niihin. Taulukon 6-1 esittämät palvelut koostuvat tiedonsiirto- , tiedostonhallinta- ja etähallintaprotokollista. Näissä olevien palveluiden haavoittuvuudet voisivat pahimmillaan antaa tunkeutujalle pääkäyttäjän oikeudet laitteistoon.

Kuvasta 6-3 nähdään, että hyökkäyksen pääosa on saapunut verkkoon kello 14:n ja 15:n välillä. Nähdään myös, että yhteysmäärä on ollut valtava. Se on selkeä merkki, että verkossa on tapahtunut jotain. Hunajapurkki on sijoitettuna käyttämättömään osoitteeseen, jolloin sille ei pitäisi tulla yhtään liikennettä.

Taulukossa 6-2 on listattu tunkeutumisen havaitsemisjärjestelmä Snortin antamat hälytykset. Huomataan, että kellonaika sopii yhteen hunajapurkin tietojen kanssa. Hälytyksistä on neljää erilaista tunnistetta. Tarkistamalla muun muassa Snort-

haavoittuvuustietokannasta saadaan selville minkälaisista uhkista on kyse [25;26;27;28]. Esimmäinen yrittää hyödyntää reitittimen haavoittuvuuksia. Tämä on outo hyökkäys Windows-hunajapurkkia kohti. Ehkä Nessus ei ole saanut täyttä selvyyttä minkä tyyppinen laite hunajapurkin pitäisi olla. Toinen hälytystunniste paljastaa sen olleen yritys ottaa Samsung-tulostinohjelmiston sisältävä laite haltuun. Kolmas tunniste kuuluu oheislaitteen haavoittuvuudelle. DUO USB-patterilaturin haavoittuvuus antaa hyökkääjän ladata ja suorittaa ohjelmia laitteella. Neljäs on yritys hyväksikäyttää Windows-käyttöjärjestelmän tiedostonjakoprotokollan haavoittuvuutta. Se kohdistuu porttiin 445, jossa hunajapurkilla on avoin portti.

Sekä Snort-hälytyksistä että Honeydsum-yhteenvedosta voidaan nähdä miltä sisäverkon laitteista hyökkäys on tullut. Ne vahvistavat toistensa epäilyjä. Huomataan, että Snort on havainnut verkossa myös toiseen koneeseen kohdistuneen hyökkäyksen. Tätä hunajapurkki ei kykene havaitsemaan, sillä se havaitsee ainoastaan sille kulkeutuvan liikenteen. Samalla tavalla Snort-sääntöjä ei voida normaaliverkossa käyttää tiukimmilla mahdollisilla säädöksillä sen aiheuttaman hälytystulvan takia, vaan voidaan tarvita vaihtoehtoista menetelmää hyökkäyksien havaitsemiseen.

Laajakaistaverkko

Laajakaistaverkkotapauksessa haluttiin tutkia verkon ulkopuolisia uhkia. Havainnointilaitteisto asetettiin reitittimen DMZ-alueelle. Snort-hälytyksiä tuli vain yksi tämän havainnointijakson aikana. Tutkittaessa ajankohtaa todettiin se vääräksi hälytykseksi. Sen aiheutti siltaavan reitittimen uudelleen käynnistyminen. On mahdollista, että jokin hyökkäys olisi aiheuttanut kyseisen häiriön laitteeseen, mutta todennäköisemmin kyse oli väärästä hälytyksestä. Reitittimen suorittama liikenteen suodatus on luultavasti karsinut DMZ-alueelle kulkeutuneesta liikenteestä sellaiset pakettikuviot, jotka aiheuttaisivat käytetyillä säännöillä Snort-hälytyksiä. Hunajapurkkiin kuitenkin saatiin paljon liikennettä. Hunajapurkkien ja tunkeutumisen havaitsemisjärjestelmien kanssa on aina tasapainoiteltava palomuurin tiukkuuden ja halutunkaltaisen liikenteen välillä. Mikäli hunajapurkille tahtoo enemmän liikennettä, on palomuurin asestuksia löysättävä ja samalla yritettävä välttää hälytystulva muiden valvontalaitteiden osalta. [8.]

Kuvasta 6-4 nähdään, että osa hunajapurkille saapuneesta tietoliikenteestä on ollut ICMP-protokollaa. Honeydsum-yhteenvedosta voidaan nähdä, että ICMP-viestit olivat 'Kohde ei ole saavutettavissa'-viestejä ja Echo-viestejä. Yleensä palomuurit estävät Echo-viesteihin vastaamisen, jotta konetta ei voida löytää sen perusteella verkossa. Ne voivat olla merkki verkonskannuksesta.

Kuvassa 6-7 on listattu käytetyimmät portit ja niiden liikennemäärät. Nähdään, että porttiin 5900 on tullut ylivoimaisesti enemmän yhteyksiä kuin muihin portteihin.

Taulukossa 6-3 se on listattu Apple-etäkäyttöohjelmiston protokollaportiksi. Taulukosta nähdään, että eniten yhteyksiä on otettu etäkäyttö- , hallinta- ja tiedonsiirtoprotokollilla. Verkkoon saapuva liikenne näyttää keskittyvän sellaisten protokollien kokeilemiseen, jotka voivat sallia tietojen kaivamisen taikka järjestelmän haltuunottamisen. Kuvasta 6-9 voidaan nähdä liikenteen keskittyvän suurelta osin yhden ja neljän väliin yöllä aikavyöhykkeellä +2. Tämä voisi viitata Pohjois-Amerikkaan, jossa noihin aikoihin on päivä meneillään.

Tarkistamalla kuvasta 6-6 kymmenen eniten yhteyksiä ottaneen lähdeosoitteen maat nähdään, että ensimmäisellä sijalla on Saksa. Kaikkiaan kymmenen suurimman joukossa on kolme yhdysvaltalaista osoitetta, yksi alankomaalainen, yksi irlantilainen, yksi venäläinen ja kaksi ranskalaista osoitetta. Tutkimalla Honeydsum-yhteenvetoa nähdään, että ne ovat pääosin keskittyneet yhteen tai kahteen porttiin yhteydenotoissaan. Näiden käyttämät portit vastaavat käytetyimpien porttien taulukossa olevia portteja.

Honeydsum-yhteenvetoa tutkimalla nähtiin, että hunajapurkille tuli yksittäisten yhteydenottojen lisäksi kahdenlaisia hyökkäyksiä. Yhden portin kuormittaminen suurella määrällä yhteydenottoja ja porttiskannauksen suorittaminen peräkkäisten tai lähekkäisten porttien kokeilemisella. Kuvasta 6-8 nähdään, että laajoja skannauksia ei verkossa tehty. Maantieteelliseltä sijainniltaan lähdeosoitteet sijoittuvat pääosin Eurooppaan.

Matkapuhelinverkko

Hunajapurkki ja tunkeutumisen havaitsemisjärjestelmä sijoitettiin matkapuhelinverkkoon liittyneen reittimen DMZ-alueelle ja palomuuri poistettiin käytöstä. Havainnointijakson aikana hunajapurkkiin tuli paljon liikennettä. Taulukosta 6-4 nähdään, että yhteydenotot koostuivat pääosin etäkäyttö- , tiedonsiirto- ja tiedostonhallintaprotokollista. Kolmen kärkenä olivat Microsoft-päätepalvelin, VNC-etäkäyttöprotokolla ja SSH-salattu tietoliikenneprotokolla. Ne etsivät verkosta haavoittuvuuksia, jotka sallisivat laitteiden haltuunottamisen.

Joukossa on myös tietokantapalvelin ja IRC-palvelin. Tietokannat ovat kiinnostava kohde, koska sellaisen löydyttyä oletusportista voidaan yrittää päästä käsiksi tärkeisiin tietoihin. IRC-palvelin on kauan tunnettu haavoittuvaiseksi hyökkäyksille.

Porttiin 18662 tuli myös kohtalaisesti yhteyden ottoja. Sille ei ole tiedossa virallista eikä epävirallista mutta suosittua palvelua. On mahdollista, että se on jonkin vähemmän käytetyn ohjelmiston oletusportti ja siksi sille tulee liikennettä.

Kuvasta 6-15 nähdään, että liikenne ajoittuu kello 10:n ja 12:n välille aamupäivällä, sekä kello 22:n ja 1:n välille yöllä. Se voi viitata, että liikennettä on tullut kahdelta eri alueelta. Kun kuvassa 6-12 verrataan vilkkaimpien lähdeosoitteiden maantieteellisiä sijainteja nähdään, että Kiinasta ja Venäjältä molemmista oli kaksi osoitetta.

Argentiinasta on tullut määrällisesti eniten yhteydenottoja. Myös Romania, Yhdysvallat, Ranska, Alankomaat ja Ruotsi ovat eniten yhdistäneiden joukossa. Nämä voidaan lajitella Amerikan mantereisiin, Eurooppaan ja Aasiaan lähdealueiden tai aikavyöhykkeiden perusteella.

Kuvasta 6-14 nähdään, että verkkoon on kohdistettu muutamia laajoja skannauksia, joissa on käyty useita peräkkäisiä portteja lävitse. Suurimmat porttiskannaukset tulivat Yhdysvalloista ja Saksasta. Puolet kuvan porttiskannauksien lähdeosoitteista on yhdysvaltalaisia. Lisäksi Kiinasta, Etelä-Afrikasta, Islannista ja Alankomaista on tullut porttiskannauksia.

Taulukosta 6-5 nähdään, että Snort on hälyttänyt yksitoista kertaa. Haavoittuvuustietokannoista tarkistamalla nähdään, että kyseessä on Lovegate-matoja ja Microsoft RPC DCOM-palvelun haavoittuvuuden hyväksikäyttöyrityksiä [23;24]. Selvitettämällä hälytyksiä vastaavat maantieteelliset sijainnit nähdään, että jokainen niistä on tullut Saksan Hampurista. Kyseessä voi olla yksittäinen kone, jonka IP-osoitetta vaihdetaan aina tietyin väliajoin taikka se voi olla jokin pieni verkko, joka on saastunut.

Virtuaalipalvelin

Virtuaalipalvelintapauksessa jäljiteltiin sisäverkkoa, jonka koneita yhdistetään Internetiin käyttäen virtuaalipalvelimelle määriteltyjä reittejä. Liikennettä hunajapurkille tuli huomattavasti vähemmän kuin reitittimen DMZ-alueelle sijoitettuihin hunajapurkkeihin edellisissä tapauksissa. Tämä ei ollut yllättävää sillä ainoastaan itse määritellyt yhteydet pääsevät hunajapurkille asti.

Kuvista 6-18 ja 6-19 on heti selvää, että verkossa on ollut jotain erikoista. Molemmissa kuvaajissa on yksittäisen lähdeosoitteen kohdalla suuri piikki. Voidaan kuvasta 6-20 nähdä, että selkeästi suurin määrä liikennettä on kulkenut porttiin 143. Se on sähköpostien lukemiseen tarkoitettu IMAP-protokolla ja hunajapurkki oli asetettu jäljittelemään sen palvelua kyseisessä portissa. Tämän hyökkäyksen tarkoituksena oli yritää hyödyntää protokollassa olevia heikkouksia. Kuvan 6-22 tuntijaosta nähdään liikenteessä selkeä piikki kello seitsemän ja kahdeksan välissä. Tutkimalla hunajapurkin lokitiedostoa nähdään, että kyseisessä osoitteessa on Windows XP SP1-kone. Se on lähettänyt 556 yhteyden ottoa 143 porttiin puolen tunnin pituisessa jaksossa, jonka jälkeen se hiljeni täysin. Tarkastamalla lähdeosoitteen maantieteellisen sijainnin nähdään, että liikenne on peräisin Brasiliasta.

Tämän lisäksi vilkkaimmista lähdeosoitteista yksi oli serbialainen, kaksi suomalaista, yksi brasilialainen, yksi saksalainen, kolme yhdysvaltalaista ja yksi kanadalainen. Liikennettä tuli lähinnä tiedostonjako- , etähallinta- ja tiedonsiirtoprotokollille. Niiden haavoittuvuuksia hyödyntämällä voitaisiin yrittää saada verkonlaitteistoa hallintaan.

Yksikään taulukon 6-6 Snort-hälytyksistä ei ollut tullut yllä mainitusta brasilialaisesta osoitteesta. Mielenkiintoisesti hälytysten lähdeosoitteista kolme sijoittuu Suomeen ja kaksi sijoittuvat puolestaan Saksaan. Tarkastamalla hälytysten tunnisteet haavoittuvuustietokannoista saadaan selville, että verkossa on havaittu Lovegate-matoja ja Microsoft RPC DCOM-palvelun haavoittuvuuden hyväksikäyttöyrityksiä [23;24]. Näiden tavoitteena on saada kohdejärjestelmä hallintaan tai saastutettua madolla. Ne ovat Windows-käyttöjärjestelmää vastaan kohdistettuja haavoittuvuuksien hyväksikäyttöyrityksiä.

Kuvasta 6-21 nähdään verkkoon kohdistettujen porttiskannausten olleen rajoittuneita. Tämä johtuu siitä, että virtuaalipalvelimella ohjataan liikenne tiettyihin portteihin, jolloin porttiskannausten yhteydenottoyritykset muihin kuin reititettyihin portteihin eivät koskaan kulkeudu hunajapurkille. Eniten eri porttinumeroita on kokeiltu Suomesta, sitten kahdesta Yhdysvaltalaisesta osoitteesta. Voidaan sanoa, että virtuaalipalvelimen takana hunajapurkki on suojassa porttiskannauksilta. Se estää hyökkäjiä saamasta tietoa verkonrakenteesta ja pääsemästä käsiksi turvaamattomiin palveluihin.

Hunajaverkko

Tässä havainnointijaksossa ohjattiin liikenne matkapuhelinverkosta virtuaalipalvelimen kautta hunajapurkeille. Yhteensä liikennettä ei ollut kovin suurta määrää, mikä johtui siitä, että verkko oli palomuurin suojaama ja ulkoverkon liikenne oli reititetty portteihin. Liikenne oli siis rajoittunut niihin portteihin ja palveluihin, jotka ennalta määriteltiin.

Windows 2000 Server-hunajapurkkiin tuli toiseksi eniten liikennettä. Taulukosta 6-8 nähdään, että havainnointijaksolla tuli kaksikymmentäneljä Snort-hälytystä. Niistä kaksitoista olivat 9423 tunnisteella ja toiset kaksitoista olivat 3397 tunnisteella. Haavoittuvuustietokannoista tarkastamalla nähdään, että ne viittaavat Lovegate-matoon ja Microsoft RPC DCOM-palvelun haavoittuvuuden hyväksikäyttöyritykseen [23;24]. Snort-ohjelman havaitsemat hyökkäykset olivat suunnattu Windows 2000 Server-palvelinhunajapurkille. Tarkasteltaessa lähdeosoitteiden maantieteellistä sijaintia huomataan, että ne olivat Euroopasta. Yhteyksiä tuli Puolasta, Belgiasta, Espanjasta, Unkarista, Romaniasta, Saksasta, Itävallasta ja Turkista.

Linux-hunajapurkille tuli vähiten liikennettä. Sen yhteydet sijoittuvat ympäri maailmaa. Näin pienestä määrästä liikennettä ei voida vetää muita johtopäätöksiä kuin, että kaikki kutsumaton liikenne on epäilyksen alaista.

Tämän havainnointijakson hunajapurkeista Cisco-reitittimelle tuli eniten yhteydenottoja. Kaikki sille saapuneet yhteydenotot kokeilivat portissa 23 jäljiteltävää telnet-palvelua, koska se oli ainoa Cisco-reitittimelle virtuaalipalvelimelta ohjattu yhteys.

Kokonaisuudessaan hunajaverkkoon saapui vain vähän liikennettä. Tämä johtuu siitä, että verkko on palomuurin suojaama ja sille johdetaan matkapuhelinverkosta ainoastaan virtuaalipalvelimelle määritelty liikenne. Muutamasta lähdeosoitteesta saapui hieman enemmän liikennettä kuin muista. Kuvasta 6-29 nähdään, että kaksi selvästi erottuvaa protokollaa olivat 23 ja 135. Portissa 23 oli telnet-palvelin. Porttiin 135 kulkevat Microsoft EPMAP-protokollan yhteysyritykset. Sitä käytetään palvelujen etäkäyttöön. Voidaan epäillä näitä kokeiluyrityksiksi.

Kuvassa 6-30 tietoliikenne on jaettu vuorokauden tunneille. Voidaan nähdä kolme huippua. Ensimmäinen on puolenyön ja kolmen välissä, toinen on kahdeksan ja kahdentoista välillä aamulla ja kolmas on hajanainen huippu, jonka liikennöinti on jakaantunut koko illan ajaksi. Kellon ajoista voidaan päätellä liikenteen saattaneen olla kolmelta erilliseltä aikavyöhykkeeltä. Kuvasta 6-28 nähdään, että vilkkaimpien lähdeosoitteiden joukko on jakaantunut maailmalle. Niistä Yksi on Kiinasta, kolme on Ruotsista, yksi Portugalista, yksi Itävallasta, yksi Iso-Britanniasta, yksi Meksikosta, yksi Chilestä ja yksi Alankomaista.

7 YHTEENVETO

Tutkimuksessa haluttiin selvittää hunajapurkkien ja tunkeutumisen havaitsemisjärjestelmän käyttöä verkon tarkkailussa. Toteutettiin viisi erilaista verkkotapausta ja niiden avulla havainnotiin verkkoliikennettä. Ensimmäisessä tehtiin sisäverkossa haavoittuvuusskannaus, jolla jäljiteltiin sisäverkkoon päässyttä uhkatekijää. Toisessa tarkkailtiin ADSL-yhteydellä Internetiin yhdistetyn reitittimen DMZ-aluetta. Kolmannessa tarkkailtiin matkapuhelinverkkoon liitetyn reittittimen DMZ-aluetta. Neljännessä reitittimen virtuaalipalvelimella ohjattiin matkapuhelinverkosta tulevaa liikennettä hunajapurkkien tarjoamiin palveluihin. Viidennessä tarkasteltiin hunajaverkkoa, jonne liikenne ohjattiin virtuaalipalvelimella matkapuhelinverkosta.

Verkon havainnoinin tuloksista voidaan todeta, että hunajapurkeilla voidaan havaita erilaisia hyökkäyksiä ja ne voidaan sijoittaa verkkoon eri tavalla kuin tunkeutumisen havaitsemisjärjestelmä. Siinä missä tunkeutumisen havaitsemisjärjestelmä etsii mahdollisia hyökkääjiä havainnoimalla verkossa kulkevaa liikennettä, hunajapurkki perustuu siihen, että hyökkääjä löytää sen. Molempia järjestelmiä voidaan käyttää yhteistyössä verkon turvaamiseksi. Tunkeutumisen havaitsemisjärjestelmä voidaan sijoittaa tarkkailemaan Internet-yhteyskohtia, joiden kautta koko verkon liikenne kulkee. Hunajapurkkeja voidaan sijoittaa verkon eri osiin muiden verkon laitteiden rinnalle, jolloin ne havaitsevat verkon sisäisiä skannauksia ja yhteysyrityksiä.

Verkkotapauksista saatiin hunajapurkin ja tunkeutumisen havaitsemisjärjestelmän sijoitus paikasta ja verkon rakenteesta riippuvia tuloksia. Snort-hälytyksiä saatiin vähemmän kuin olisi voinut odottaa varsinkin suojaamattomissa yhteyksissä. Tämä on voinut johtua käytetyistä havaitsemisjärjestelmän sääntöjen löyhyydestä, verkon rakenteesta tai hyökkäysten vakavuuden jäämisestä raja-arvojen alle. Hunajapurkeilta kerätystä lokitiedosta voitiin todeta useita hyökkäyksiä, joita Snort ei ilmoittanut.

Sisäverkkotapauksessa onnistuttiin skannauksen käyttämiä hyökkäyksiä havaitsemaan niin tunkeutumisen havaitsemisjärjestelmällä kuin hunajapurkkillakin. Tämä osoittaa, että toteutettu asetelma oli toimiva. Kokonainen haavoittuvuusskannaus aiheutti hunajapurkille valtavasti lokitietoa, jonka perusteella voitaisiin skannausta suorittava laite löytää verkosta. Snort-hälytyksiä tutkimalla kyettäisiin myös näkemään skannausta suorittava kone ja myös minkälaisia hyökkäyksiä skannauksen lisäksi on käytetty. Näiden perusteella voitaisiin ryhtyä toimenpiteisiin tietoturvauhkan poistamiseksi. Vaikka sisäinen hyökkääjä käyttäisi huomaamattomampia keinoja verkon

rakenteen hahmottamiseen, niin hunajapurkille saapuvasta yhteydenotosta heräisi aina epäilys. Sisäverkkojen tietoturvan tutkiminen on tärkeää, sillä huomaamattomana tai liian myöhään huomattuna voivat esimerkiksi yritykselle koituvat menetykset olla suuria. Lisätutkimukseksi voitaisiin tehdä useita erilaisia hyökkäyksiä käyttäen turvallisuustestaajien työkalupakkeja. Voitaisiin myös testata hyökkäyksen havaitsemista käyttäen hajautettua tunkeutumisen havaitsemisjärjestelmää.

Laajakaistaverkkotapauksessa yhdistettiin Internetiin ADSL-yhteyden kautta. Siitä saadut tulokset olivat ristiriitaisia. Hunajapurkki havaitsi jatkuvasti yhteydenottoja ja sen lokitiedostoista nähdään, että joukossa on ollut lyhyitä porttiskannauksia, mutta tunkeutumisen havaitsemisjärjestelmä ei antanut hälytyksiä. Syynä on voinut olla verkon rakenne, reitittimen asetukset, operaattorin suorittamat toimenpiteet verkossa tai rauhallinen ajanjakso liikenteessä. Voidaan kuitenkin todeta, että DMZ-alueelle sijoitettu hunajapurkki toimisi anturina siitä liikenteestä, jota muille samalle alueelle sijoitetuille laitteille tulisi. Jatkotutkimuksessa voitaisiin keskittyä enemmän tunkeutumisen havaitsemisjärjestelmien toiminnan tutkimiseen. Kiinnostavaa olisi Internetin eri osiin hajautetun mukautuvan tunkeutumisen havaitsemisjärjestelmän tutkiminen ja sen mahdollisuuksien kartoittaminen.

Matkapuhelinverkkotapauksessa liikenteen tuloksissa ei ollut paljoa eroa perinteiseen ADSL-yhteyteen. Suurin ero huomattiin siinä, että matkapuhelinverkon kautta tuli selkeitä hyökkäyksiä, joihin tunkeutumisen havaitsemisjärjestelmä Snort reagoi, kun taas ADSL-yhteyden kautta näitä ei tullut. Havaintojakson lyhyydestä johtuen ei voida vetää tarkkoja johtopäätösiä matkapuhelinverkon turvallisuudesta, mutta voidaan todeta, että matkapuhelinverkot vaikuttavat olevan yhtä turvattomia kuin ADSL-yhteydet. Tulevaisuudessa matkapuhelinverkkoa käyttävien laitteiden määrä on kasvussa, joten voidaan ennustaa niiden kautta tulevien hyökkäysten kasvavan. Tarkempia tuloksia saataisiin suorittamalla pitkäaikainen tarkastelujakso. Lisäksi voitaisiin käyttää tutkimuksessa esimerkiksi Android käyttöjärjestelmällä varustettuja laitteita, jolloin saataisiin parempi kuva kannettavien laitteiden tilasta.

Virtuaalipalvelintapauksessa tulokset olivat selkeitä, mutta vähäisiä. Niiden määrä oli pieni, koska virtuaalikone ohjasi ainoastaan sille määritellyt yhteydet hunajapurkeille. Verrattaessa liikenteen määrää esimerkiksi laajakaistaverkkotapauksessa saapuneeseen määrään, voidaan nähdä, että virtuaalipalvelinta voidaan käyttää tehokkaasti suojaamaan laitteita ylimääräiseltä altistukselta hyökkäyksille. Rajoitetusta pääsystä huolimatta hunajapurkeille tuli hyökkäyksiä. On siis tärkeää suojata sallitut palvelut silloinkin, kun niitä ei käytetä.

Hunajaverkkotapaus oli virtuaalipalvelintapauksen laajennus, jossa hunajapurkkeija oli yhden sijasta kolme. Hunajaverkkoon tullut liikenne jakaantui epätasaisesti eri laitteille. Voidaan sanoa, että hunajaverkko toimii hyvin oikean verkon jäljitelmänä. Virtuaalipalvelimen käyttämisestä liikenteen ohjaamiseen hunajapurkeille johtuen

liikennettä ei tullut suurta määrää, mutta nähdään, että verkkona se toimii. Tämä voitaisiin toteuttaa laajakaistaverkkotapauksessa, jolloin liikennemäärät kasvaisivat merkittävämmiksi. Kuten virtuaalipalvelintapauksessa tässäkin hyökkäyksiä saapui avattuihin portteihin ja verkon suojaamiseksi on tärkeää, että niitä suojataan, kun niissä käytettävät palvelut eivät ole käytössä. Yksi mahdollinen lisätutkimuskohde voisi tutkia kotien Internet-yhteydellisen elektroniikan, kuten konsoleiden, televisioiden ja niiden palveluiden turvallisuutta. Internet-yhteydet ja laitteiden älykkyys tulee lisääntymään jatkuvasti myös kaikissa kodin laitteissa ja niiden suojana on yleensä palomuuri. Kuitenkin laitteet tarvitsevat usein päivityksiä ja Internet-palveluita, jolloin palomuuriin on tehtävä reikiä ja ohjattava liikenne oikeisiin portteihin.

Jatkotutkimuksissa olisi hyvä käyttää pidempiä havainnointijaksoja, jolloin niistä saadut tulokset ovat kattavampia. Myös verkossa käytetyn tunkeutumisen havaitsemisjärjestelmän asetuksiin ja sijaintiin on syytä kiinnittää erityistä huomiota. Asetukset vaikuttavat, kuinka paljon oikeita ja vääriä hälytyksiä saadaan. Sijainti määrittelee minkälainen liikenne havainnointijärjestelmälle kulkee.

LÄHTEET

[1] Provos, N. & Holz, T. 2008. Virtual honeypots. 1.painos. Stoughton, Massachusetts, Addison-Wesley. 440s.

[2] Bejtlich, R. 2005. Extrusion detection. 1. painos. Westford, Massachusetts, Addison-Wesley. 385s.

[3] Rehman, R. U. 2003. Intrusion detection with Snort. 4. painos. Yhdysvallat, Prentice Hall PTR. 263s.

[4] Stallings, W. 2002. Network Security Essentials. 2.e. 10. painos. Yhdysvallat, Prentice Hall. 409s.

[5] European Network Information Agency. 2012. [PDF]. [viitattu 20.12.2012]. Saatavissa: http://www.enisa.europa.eu/activities /cert/support/proactive-detection-of-security-incidents-II-honeypots /at_download/fullReport

[6] Allen J. H. 2002. Verkkotietoturvan hallinta- CERT. Suomenkielinen versio, Suomi, Helsinki, Edita Prima Oy, IT Press. 438s.

[7] Hakala M. & Vainio M. & Vuorinen O. 2006. Tietoturvallisuuden käsikirja. 2. painos. Suomi, Porvoo, Docendo Finland Oy, WS Bookwell. 422s.

[8] Stallings, W. & Brown, L. 2012. Computer Security Principles And Practice. 2.e. USA. Pearson Education Limited. 810s.

[9] dd-wrt. 2012. [WWW]. [viitattu 6.5.2013]. http://www.dd-wrt.com/wiki/index.php/installation

[10] Järvinen, P. 2006. Paranna Tietoturvaasi. Suomi, Porvoo, Docendo Finland Oy, WS Bookwell. 352s.

[11] Snort. 2013. [viitattu 15.1.2013]. [FILE]. http://www.snort.org/downloads/2334

[12] Tenable Network Security. 2013. Nessus. [viitattu 6.5.2013]. [PDF]. https://static.tenable.com/datasheets/nessus-datasheets.pdf

[13] Symmetrix Technologies. 2012. [viitattu 10.5.2013]. [FILE]. http://www.symmetrixtech.com/download.html

[14] Firns, I. 2013. [FILE]. [viitattu 6.5.2013]. https://github.com/firnsy/barnyard2

[15] Firns, I. 2013. README. [WWW]. [viitattu 6.5.2013]. https://github.com/firnsy/barnyard2/blob/master/README

[16] Ubuntu manuals. 2010. farpd. [WWW]. [viitattu 6.5.2013]. http://manpages.ubuntu.com/manpages/precise/man8/farpd.8.html

[17] Ubuntu manuals. 2010. Snort. [WWW]. [viitattu 6.5.2013]. http://manpages.ubuntu.com/manpages/precise/en/man8/snort.8.html

[18] Ubuntu manuals. 2010. MySQL [WWW]. [viitattu 6.5.2013]. http://manpages.ubuntu.com/manpages/precise/en/man1/mysql.1.html

[19] Snort. 2012. [PDF]. [Viitattu 13.02.2013]. http://www.snort.org/assets/158/snortinstallguide293.pdf

[20] Symantec Corporation. 2012. [WWW]. [viitattu 27.4.2013]. http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year&=suid=20120124_00

[21] Microsoft Security Bulletin. 2012. [WWW]. [viitattu 27.4.2013]. http://technet.microsoft.com/en-us/security/bulletin/ms12-020

[22] Snort. 2013. [WWW]. [viitattu 28.4.2013]. http://www.snort.org/search/sid/15699

[23] Snort. 2013. [WWW]. [viitattu 28.4.2013]. http://www.snort.org/search/sid/9423

[24] Snort. 2013. [WWW]. [viitattu 28.4.2013]. http://www.snort.org/search/sid/3397

[25] OSVDB: The Open Source Vulnerability Database. 2005. [WWW]. [viitattu 28.4.2013]. http://osvdb.org/18753

[26] Snort. 2013. [WWW]. [viitattu 28.4.2013]. http://www.snort.org/search/sid/16487

[27] Snort. 2013. [WWW]. [viitattu 28.4.2013]. http://www.snort.org/search/sid/15930

[28] Vulnerability Notes Database. 2012. [WWW]. [viitattu 28.4.2013]. http://www.kb.cert.org/vuls/id/281284

[29] Chandran, R & Pakala, S. Simple Network Template. 2003. [WWW]. [viitattu 6.5.2013]. http://www.honeyd.org/config/honeyd.conf.networks

[30] Snort. 2013. [WWW]. [viitattu 4.5.2013]. http://www.snort.org/

[31] MySQL. 2013. [WWW]. [viitattu 10.5.2013]. http://dev.mysql.com/downloads/mysql/

LIITTEET:

Liite 1. Ohjelmistojen Snort, MySQL, Barnyard2 ja Snort Report asennus:

Tässä liitteessä esitettyihin asennuksiin käytetty ohjelmistojen päivitettyjä versioita asennusohjeesta [19.].

Asennuksessa tarvittavat paketit:

```
sudo apt-get install nmap
sudo apt-get install nbtscan
sudo apt-get install apache2
sudo apt-get install php5
sudo apt-get install php5-mysql
sudo apt-get install php-gd
sudo apt-get install libpcap0.8-dev
sudo apt-get install libpcre3dev
sudo apt-get install g++
sudo apt-get install bison
sudo apt-get install flex
sudo apt-get install libpcap-ruby
sudo apt-get install make
sudo apt-get install autoconf
sudo apt-get install libtool
```

MySQL:n asennus:

```
sudo apt-get install mysql-server
sudo apt-get install libmysqlclient-dev
```

Ubuntun päivittäminen:

```
sudo apt-get update
sudo apt-get upgrade
```

Snort Reportin asennus:

```
sudo tar zxvf snortreport-1.3.3.tar.gz -C /var/www/
sudo vi /var/www/snortreport-1.3.3/srconf.php
$pass = "YOURPASSWORD";
```

Snortin asennus:

Ladataan ja asennetaan Data Acquisition API-rajapinta

```
sudo tar zxvf daq-1.1.1.tar.gz
cd daq-1.1.1
sudo ./configure
```

sudo make
sudo make install

Ladataan ja asennetaan libdnet:
sudo tar zxvf libdnet-1.12.tgz
cd libdnet-1.12/
sudo ./configure
sudo make
sudo make install
sudo ln -s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1

Ladataan ja asennetaan Snort:
sudo tar zxvf snort-2.9.4.tar.gz
cd snort-2.9.4
sudo ./configure –prefix=/usr/local/snort --enable-sourcefire
sudo make
sudo make install
sudo mkdir /var/log/snort
sudo mkdir /var/snort
sudo groupadd snort
sudo useradd -g snort snort
sudo chown snort:snort /var/log/snort

Ladataan viimeisimmät dynaamiset säännöt osoiteesta:
http://www.snort.org/snort-rules/

sudo tar zxvf snortrules-snapshot-2940.tar.gz-C /usr/local/snort
sudo mkdir /usr/local/snort/lib/snort_dynamicrules
sudo cp /usr/local/snort/so_rules/precompiled/Ubuntu-12-04/i386/2.9.4.0/* \
/usr/local/snort/lib/snort_dynamicrules
sudo touch /usr/local/snort/rules/white_list.rules
sudo touch /usr/local/snort/rules/black_list.rules
sudo ldconfig

Muokataan tiedostosta /usr/local/snort/etc/snort.conf seuraavien rivien polut:
var WHITE_LIST_PATH /usr/local/snort/rules
var BLACK_LIST_PATH /usr/local/snort/rules

dynamicpreprocessor directory /usr/local/snort/lib/snort_dynamicpreprocessor/

dynamicengine /usr/local/snort/lib/snort_dynamicengine/libsf_engine.so
dynamicdetection directory /usr/local/snort/lib/snort_dynamicrules

Lisätään seuraava rivi:
output unified2: filename snort.u2, limit 128

Ladataan ja asennetaan Barnyard2:
wget https://github.com/firnsy/barnyard2/archive/master.tar.gz

sudo tar zxvf master.tar.gz
cd barnyard2-master
sudo autoreconf-fvi-I ./m4
sudo ./configure –with-mysql --with-mysql-libraries=/usr/lib/i386-linux-gnu
sudo make
sudo make install
sudo cp etc/barnyard2.conf /usr/local/snort/etc
sudo mkdir /var/log/barnyard2
sudo chmod 666 /var/log/barnyard2
sudo touch /var/log/snort/barnyard2.waldo
sudo chown snort.snort /var/log/snort/barnyard2.waldo

Luodaan MySQL-tietokanta ja tietokantaskeema:
echo "create database snort;" | mysql -u root -p
mysql -u root -p -D snort < ./schemas/create_mysql

echo "grant create, insert, select, delete, update on snort.* to snort@localhost \
identified by 'honeysnort'" | mysql -u root -p

Muokataan seuraavaa tiedostoa:
/usr/local/snort/etc/barnyard2.conf

Muutetaan tiedoston vastaavat rivit seuraavan kaltaisiksi:
config reference_file: /usr/local/snort/etc/reference.config
config classification_file: /usr/local/snort/etc/classification.config
config gen_file: /usr/local/snort/etc/gen-msg.map
config sid_file: /usr/local/snort/etc/sid-msg.map

config hostname: localhost
config interface: eth0

output database: log, mysql, user=snort password=YOURPASSWORD
dbname=snort host=localhost

Asetetaan verkkokortit muokkaamalla tiedostoa:
/etc/network/interfaces

Muokataan tiedosto seuraavan kaltaiseksi:
auto eth0
iface eth0 inet static
address 192.168.1.1
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
auto eth1
iface eth1 inet manual
ifconfig eth1 up

Käynnistetään tietokone uudestaan tai käytetään seuraavaa komentoa:
sudo /etc/init.d/networking restart

Snortin käynnistäminen:
sudo /usr/local/snort/bin/snort -u snort -g snort
-c /usr/local/snort/etc/snort.conf -i eth0

Barnyard2:n käynnistäminen:
sudo /usr/local/bin/barnyard2 -c /usr/local/snort/etc/gen-msg.map -S
/usr/local/snort/etc/sid-msg.map -d /var/log/snort/-f snort.u2 -u
/var/log/snort/barnyard2.waldo

Snortin ja Barnyardin automaattinen käynnistäminen:
Lisätään tiedostoon /etc/rc.local seuraavat rivit ennen exit 0-riviä:

ifconfig eth1 up
/usr/local/snort/bin/snort -D -u snort -g snort
-c /usr/local/snort/etc/snort.conf -i eth1
/usr/local/bin/barnyard2 -c /usr/local/snort/etc/barnyard2.conf
-G /usr/local/snort/etc/gen-msg.map
-S /usr/local/snort/etc/sid-msg.map

-d /var/log/snort
-f snort.u2
-w /var/log/snort/barnyard2.waldo
-D

Tallennetaan muutokset ja uudelleen käynnistetään tietokone taikka käytetään seuraavaa komentoa Snortin käynnistämiseksi:
sudo /etc/init.d/rc.local start

Snort Report-ohjelman etusivu selaimessa:
localhost/snortreport-1.3.3/alerts.php

Liite 2: Ohjelmistojen Honeyd ja farpd asennus

Noudetaan ja asennetaan Honeyd:
git clone git://github.com/Datasoft/honeyd.git
git checkout -f integration
./autogen.sh
automake
./configure
make -j2
make install

farpdin asennus:
sudo apt-get install farpd

Muokataan tiedostoa
/etc/default/farpd

Asetetaan verkkoliitännäksi
INTERFACE=”eth0”

Asetetaan luotaviksi osoitteiksi hunajapurkkien osoitteet
NETWORK=”10.0.0.101”
Tähän voidaan määrittää myös useita osoitteita taikka kokonainen verkko.

Käynnistetään farpd uudelleen
sudo /etc/init.d/farpd restart

Liite 3: Honeyd hunajapurkkien asetustiedostot:

Sisäverkko, laajakaistaverkko, matkapuhelinverkko ja virtuaalipalvelin käyttävät samaa hunajapurkki asetelmaa. Ainoana erona on, että hunajapurkin osoite vaihtuu verkkoon sopivaksi:

```
create default
set default default tcp action block
set default default udp action block
set default default icmp action block

### Windows 2000 server sp4 windows
create windows
set windows personality "Microsoft Windows 2000 Server SP4"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "sh scripts/win32/win2k/iis.sh"
add windows tcp port 110 "sh scripts/win32/win2k/exchange-pop3.sh"
add windows tcp port 25 "sh scripts/win32/win2k/exchange-smtp.sh"
add windows tcp port 21 "sh scripts/win32/win2k/msftp.sh"
add windows tcp port 23 open
add windows tcp port 143 "sh scripts/win32/win2k/exchange-imap.sh"
add windows tcp port 139 open
add windows tcp port 138 open
add windows udp port 138 open
add windows tcp port 137 open
add windows udp port 137 open
add windows udp port 135 open
add windows tcp port 445 open
add windows udp port 445 open
set windows uptime 145578
bind 192.168.0.117 windows
```

Hunajaverkko:

```
Mukailee asetuspohjaa [29.].
create default
set default default tcp action block
set default default udp action block
set default default icmp action block
### Windows win2k server sp4 windows
create windows
set windows personality "Microsoft Windows 2000 Server SP4"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "sh scripts/win32/win2k/iis.sh"
add windows tcp port 139 open
add windows tcp port 137 open
add windows udp port 137 open
add windows udp port 135 open
set windows uptime 2345990
bind 192.168.1.111 windows
### Linux 2.4.20 linux
create linux
set linux personality "Linux 2.4.20"
set linux default tcp action reset
set linux default udp action reset
add linux tcp port 25 "sh scripts/unix/general/smtp.sh"
add linux tcp port 21 "sh scripts/linux/ftp.sh"
add linux tcp port 445 open
add linux tcp port 110 "sh scripts/unix/general/pop/pop3.sh"
set linux uptime 4233480
bind 192.168.1.112 linux
### Cisco 2500 router
create router
set router personality "Cisco 2500 router (IOS 11.1)"
set router default tcp action reset
set router default udp action reset
add router tcp port 23 "perl scripts/embedded/router-telnet.pl"
set router uid 35464 gid 35464
set router uptime 1226420
bind 192.168.1.113 router
```